1&1 Internet AG

Hauptstadtbüro
Neustädtische Kirchstraße 8
10117 Berlin
Fon +49 30 8103152-8821
Fax +49 30 8103152-8822
hauptstadtbuero@1und1.de

Kurzbewertung zu einzelnen zentralen Aspekten des Entwurfs zur EU-Datenschutz-Grundverordnung aus Sicht der 1&1 Internet AG

offizieller Entwurf der Kommission vom 25. Januar 2012

I. "Level playing field" der Regulierung

- Der Ansatz der Kommission, eine **Harmonisierung** des Datenschutzrechts in Europa und bessere Anwendbarkeit und Durchsetzbarkeit auch gegenüber Anbietern aus Drittstaaten sicherzustellen, ist begrüßenswert und wird den Wettbewerb stärken.
- Der **Verordnungscharakter** trägt zu diesem Ziel bei und verdient Unterstützung – Mitgliedsstaaten sollten jedoch einen genauen Blick auf die nachgelagerten Befugnisse (delegated & implementing acts) haben und die dort gegebenen Einflussmöglichkeiten wahrnehmen.
- Die Einführung eines **„Marktortprinzips" (Art. 3 Abs. 2)** zur Sicherstellung der Anwendbarkeit europäischen Rechts auch gegenüber Anbietern aus Drittstaaten ist begrüßenswert und sollte auf jeden Fall erhalten bleiben.
- Die Regelungen zur **Sicherstellung einer einheitlicheren Durchsetzungspraxis** der Datenschutzbehörden in den Abschnitten Kapitel 7 Sektion 1 & 2 (cooperation & consistency, Art. 55 – 63) sind zu begrüßen. Allerdings sollten angesichts der Tragweite der in diesem Rahmen vorzunehmenden Auslegungsentscheidungen neben der Kommission auch die Mitgliedstaaten sowie die von Regelungen Betroffenen, also Nutzer & Wirtschaft, in das Verfahren eingebunden sein.
- Im Hinblick auf die **Zuständigkeitsregelung** des Art. 51 Abs. 2 für Unternehmen mit Sitz in Europa stellt sich die Frage, welche Datenschutzbehörde in den Fällen des Art. 3 Abs. 2 (Anbieter aus Drittstaaten) zuständig sein soll. Dieser Fall scheint bislang nicht geregelt. Begrüßenswert wäre entweder eine parallele Zuständigkeit aller europäischen DPA oder eine zentral normierte Zuständigkeit - ggf. sogar angesiedelt bei EU
- Als problematisch erscheinen die Regelungen zum sog. **Angemessenheitsbeschluss** (Art. 41, „**safe harbor**"-Abkommen), die bisher schon ausgenutzt wurden, um das europäische Datenschutzniveau zu unterlaufen. Hier besteht die Gefahr, dass sich Unternehmen durch diese Hintertür der Anwendung der VO und insbesondere auch der Pflicht zur Benennung eines europäischen Repräsentanten entziehen.

FAZIT: ***Die 1&1 Internet AG unterstützt die mit dem Entwurf verbundenen Harmonisierungsbestrebungen im innereuropäischen Rahmen wie auch gegenüber Anbietern aus Drittstaaten. Sichergestellt werden muss indes, dass dies konsequent umgesetzt wird und insbesondere in der Praxis nicht durch die Regelungen zum sog. Angemessenheitsbeschluss (Art. 41; sog. „safe harbor"-Abkommen) unterhöhlt wird.***

II. Falsche Anreizwirkung des vollständig einwilligungszentrierten Systems

- Die Entwürfe legen ein strikt **einwilligungszentriertes System** zugrunde, das infolge der sehr umfassenden Definitionen der „betroffenen Person“ (Art. 4 Abs. 1) sowie der „personenbezogenen Daten“ (Art. 4 Abs. 2) extrem weit reicht und **keinerlei Differenzierung nach der Sensibilität** der konkret verarbeiteten Daten enthält.
- Beide Begrifflichkeiten sind dabei derart weit gestaltet (etwa durch Einbeziehung von „Online-Kennungen“), dass künftig nahezu **jedes Datum personenbezogen wäre**.
- Nach Art. 4 Abs. 1 würde es ausreichen, dass auch nur für **irgendeinen Dritten theoretisch die betroffene Person bestimmbar** ist (sog. absolute Theorie).
- Dies hätte zur Folge, dass für den Verarbeiter Personenbezug bereits vorliegen kann, obwohl er selbst die betroffene Person **weder identifizieren noch adressieren** kann.
- Die **Erwägungsgründe 23 & 24** greifen die Problematik zwar auf, indem klargestellt wird, dass nicht jede Online-Kennung zwangsläufig Personenbezug aufweisen muss – die Formulierung ist jedoch zu vage, um für die Praxis rechtssichere Abgrenzungen zu ermöglichen.
- **Art. 5 Abs. lit. e)** enthält gar ein Gebot, Daten in einer Form zu speichern, die Identifizierung der betroffenen Person ermöglicht. Dies kommt einem **Pseudonymisierungsverbot** gleich.

- Aus **Anbietersicht** hat dies eine problematische Anreizwirkung zur Folge:
  - Ökonomisch sinnvoll ist in einem solchen Regime eine möglichst weitgreifende Einholung der Einwilligung für möglichst jede Form der Datenverarbeitung.
  - Dagegen fallen Anreize zur **pseudonymen oder anonymen Ausgestaltung** von Produkten, im Sinne der bisher praktizierten und in Deutschland teils auch von Datenschutzbehörden zertifizierten Auflösung des Personenbezugs weg.
  - Ein solches rein einwilligungszentriertes System **begünstigt geschlossene, accountbasierte Plattformen** (vor allem ganze „Ökosysteme“), da diese im Rahmen ihres formalisierten Anbieter-Nutzer-Verhältnisses leichter Einwilligungen einholen können, als etwa eine rein werbebasierte Nachrichtenseite ohne Login-Pflicht.
  - Im Gegenzug werden jene **europäischen und vor allem deutsche Anbieter faktisch benachteiligt**, die sich unter Geltung des bisherigen Rechts gezielt durch Anonymisierung bzw. Pseudonymisierung darum bemüht haben, die Eingriffsintensität von Datenverarbeitungen entscheidend zu vermindern.

- Auch aus **Nutzersicht** hat ein solches System Nachteile:
  - Die notwendig werdende flächendeckende Einholung der Einwilligung für unterschiedlichste Eingriffskonstellationen wird den schon heute in Zweifel gezogenen **Warncharakter der Einwilligung** weiter schmälern.
  - Der durch die Einwilligungszentrierung beförderte **Trend zu geschlossenen Plattformsystemen** und die Benachteiligung von Angeboten mit rein faktischem Anbieter-Nutzerverhältnis (z.B. frei zugängliche journalistische Dienste) verstärkt die Tendenz zu weniger Wettbewerb und einer Konzentration auf einzelne große Anbieter.
  - In der Summe stünde zu erwarten, dass eher noch mehr und sensiblere Daten von Nutzern erhoben würden als bislang – da Nutzern gerade bei großen, marktmächtigen Anbietern kaum Alternativen zu Verfügung stehen.

- Die Weite des „data-subject"-Begriffs, der sich auch auf nicht individualisierbare Subjekte bezieht, birgt außerdem erhebliche Probleme bei der **Erfüllung von Transparenz- und Informationspflichten**, wenn die Nutzer vom Verarbeiter gar nicht adressierbar sind. Art. 10 greift diese Problematik auf, löst aber nicht die Frage, wie solche Pflichten vom Verarbeiter gegenüber ihm nicht bekannten Nutzern erfüllt werden sollen.

FAZIT: ***Der Entwurf sollte explizit die aus dem BDSG bekannten Kategorien der anonymisierten bzw. pseudonymisierten Daten aufgreifen und hierfür abgestufte Regelungen schaffen. Insbesondere sollte bei hinreichender Pseudonymisierung, die eine Wiederherstellung des Personenbezugs durch den Verarbeiter mit vertretbarem Aufwand verhindert, auf den Erlaubnisvorbehalt verzichtet werden. Verfahren der Anonymisierung und Pseudonymisierung können zum Gegenstand von Zertifizierungen gemacht werden.***

III. Hohe Bürokratieanforderungen

- Der Kommissionsentwurf enthält eine Reihe von Pflichten, die zum Teil durch das Erfordernis zusätzlicher Datenerhebung und -speicherung dem erklärten Ziel von mehr Datenschutz zuwiderlaufen und überdies auf eine massive **Erhöhung der Bürokratieaufwände für Anbieter** hinauslaufen. Die Wirkung benachteiligt vor allem **kleine und mittelständische Anbieter**, bei denen solche Bürokratieaufwände überproportionale Auswirkungen haben.
- Konkrete – nicht als abschließend zu verstehende – Beispiele:
  - **Neue, allgemeine, völlig unspezifische Dokumentationspflicht** für jegliche Verarbeitungsvorgänge in **Art. 28 Abs. 1,** die faktisch den Aufbau von Datenhalden überhaupt erst erzwingt.
  - **Gebot, personenbezogen Daten sachlich richtig und auf dem neuesten Stand zu halten** (Art. 5 lit. d) provoziert gerade Datensammlung und kann Nutzerinteresse an „Falschinformationen" zuwiderlaufen
  - Informations- und Transparenzpflichten gegenüber betroffenen Personen unabhängig davon, ob diese für Verarbeiter **individualisierbar oder auch nur adressierbar** sind (Art. 14, Art. 15 Abs. 1).
  - Die Datenschutzfolgeabschätzung kann ein sinnvolles Instrument sein, aber der Anwendungsbereich ist noch zu breit. Zu beachten: Die Generaldirektion InfoSoc der Kommission schätzt die **Kosten für die Folgeabschätzung pro Fall auf 14.000 € bei kleinen Unternehmen, 34.000 € bei Mittelständlern und 149.000 € für große Unternehmen!**

FAZIT: ***Dokumentations- und Informationspflichten müssen in praktikabler Weise konkretisiert werden und dürfen nicht selbst den Aufbau von Datenhalden allein zu Dokumentationszwecken nach sich ziehen. Die Datenschutzfolgeabschätzung muss Ausnahmeinstrument bleiben.***