HÄRTING

GRENZEN DER EINWILLIGUNG BEI HOCHKOMPLEXEN UND TECHNISIERTEN DATENVERARBEITUNGEN

Frederike Kollmar, MLE, Rechtsanwältin
Maya El-Auwad, Rechtsanwältin
HÄRTING Rechtsanwälte

INHALTSÜBERSICHT

- **Historie und rechtliche Grundlagen**: Welche Kritik gibt es an dem Institut der Einwilligung? Was sind die Anforderungen an eine wirksame Einwilligung?
- **Grenzen der Einwilligung**
- **Antworten**: Welche Antworten gibt die DSGVO? Und welche die Praxis?
- **Fazit**

1. Historie und Grundlagen der Einwilligung

HISTORIE

- **Die Einwilligung ist nicht neu:** Im „Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung“, dem ersten BDSG, Regelung zur Einwilligung (aber nur für Datenverarbeitungen öffentlicher Stellen)

- Mit dem Volkszählungsurteil des BVerfG und der Entwicklung des Rechts auf informationelle Selbstbestimmung: Gedanke der aktiven Betätigung der Grundrechtsausübung in Form der Einwilligung entsteht

- Auf europäischer Ebene: EU-GRCh erkennt die Einwilligung in Art. 8 Abs. 2 S. 1 für den Schutz personenbezogener Daten explizit an

HISTORIE

- Schließlich Ablösung der DS-RL durch die DSGVO: Verschärfung der gesetzlichen Anforderungen an die Einwilligung

- Grundsatz der Technikneutralität: Was ist mit Big Data, „Internet of things“ oder Machine Learning? Einwilligung möglich?

- Wie können die Betroffenen in die Lage versetzt werden, eine den berechtigten Interessen gleichwertige Abwägung ihrer eigenen Interessen mit denen des Verantwortlichen durchzuführen?

Kritik

KRITIK

- Breite Diskussion, wo die Grenzen zu ziehen seien, beispielsweise
  - *Einwilligung in Übermittlung in ein Drittland, in dem kein gleichwertiges Datenschutzniveau besteht?*
  - *Aktuell: Unwirksamkeit des Privacy Shields (EuGH-Urteil in der Rechtssache C-311/18 – Schrems II)*
- DSGVO hat diese Diskussionen im Blick gehabt: Eine Verarbeitung personenbezogener Daten aufgrund einer Einwilligung muss immer auch die in Art. 5 DSGVO niedergelegten Grundsätze erfüllen → Verantwortliche kann sich nicht von seinen datenschutzrechtlichen Pflichten einer Abwägung der sich gegenüberstehenden Interessen entledigen!

ANFORDERUNGEN AN DIE EINWILLIGUNG: KRITIK

- Nicht nur bei unübersichtlichen und intransparenten Sachverhalten (wie Drittstaaten-Transfer), sondern insbesondere bei hochkomplexen und technisierten Datenverarbeitungsprozessen zunehmend fraglich, ob die Anforderungen an die Einwilligung faktisch überhaupt erfüllt werden können
  - *Stichwort Big Data; viele Verantwortliche; etc.*
- Ist die Einwilligung als Grundlage für eine Datenverarbeitung von vornherein fragwürdig?
- Denn: Immer häufiger sind sich die Betroffenen der Tragweite ihrer Entscheidungen und der Auswirkungen, die diese auch auf ihr Persönlichkeitsrecht haben, nicht mehr bewusst und können es auch gar nicht mehr sein.
- Gefahr: Einwilligung wird zur „Fiktion“

Freiwilligkeit und Informiertheit

ANFORDERUNGEN AN DIE EINWILLIGUNG: FREIWILLIGKEIT

- **Freiwilligkeit**
  - *ohne Druck oder Zwang*
  - *echte und freie Wahl des Betroffenen*
  - *Art. 7 Abs. 4 Koppelung*

ANFORDERUNGEN AN DIE EINWILLIGUNG: INFORMIERTHEIT

- Transparenzvorgaben aus Art. 7 Abs. 2 S. 1 DSGVO
  - *verständliche und leicht zugängliche Information*
  - *in klarer und einfacher Sprache*

- Konzept der Selbstbestimmung
  - *Auswirkungen und*
  - *Tragweite der Entscheidung*

2. Grenzen der Einwilligung

Herausforderung für die Verantwortlichen

GRENZEN DER EINWILLIGUNG

- **Dient Verantwortlichen zur Legitimation von Datenverarbeitungen, jenseits gesetzlicher Grundlagen**
  - *Freiwilligkeit, Informiertheit setzt Informationen über*
    - Zwecke,
    - Empfänger (Drittstaatenübermittlungen und Gemeinsame Verantwortlichkeit),
    - potentielle Nachteile und Risiken, Widerruflichkeit
  - *Zweckbindung und Zweckänderung*
  - *Nachweisbarkeit: komplexe Verantwortlichkeits- und Betroffenenkonstellationen*
  - *Widerrufsmanagement und Löschkonzept*
  - *Nachberichtspflicht*

GRENZEN DER EINWILLIGUNG

Bad News

- *Das meiste müssen Sie eh abarbeiten!*

Grenzen individueller Entscheidungsfindung

GRENZEN DER EINWILLIGUNG

- **Dient den betroffenen Personen als aktive Grundrechtsausübung, aber**
  - *Freiwilligkeit und Informiertheit*
    - Bislang keine standardisierten Symbole der Kommission für bestimmte Verarbeitungskonstellationen
  - *Kontrolle*
    - Privacy-Paradox

GRENZEN DER EINWILLIGUNG

- **Datenethikkommission**
  - *„Überforderung“*
  - *Konsequenz: „Vertrauensverlust“*

- Unsachgemäßer Umgang mit dem Rechtsinstitut der Einwilligung wirkt letztlich innovationshemmend!
- DEK fordert AGB-rechtliche Überprüfung von Einwilligungserklärungen
  - *Kernbereichsschutz*
  - *Sittenwidrigkeit / Diskriminierung / Irreführung*

GRENZEN DER EINWILLIGUNG

- **Einwilligung als Ausdruck individueller Entscheidungsfindung vs. Kollektivität des Grundrechtsschutzes**
  - *Überforderungsgrad*
  - *Datenschutzniveau droht insgesamt abzusinken*
    - vgl. etwa Art. 9 Abs. 2 lit. a 2. HS DSGVO
    - Diskriminierungsschutz

3. Antworten der DSGVO

Anonymisierung

Ausweichen auf sonstige Rechtsgrundlagen

ANTWORTEN DER DSGVO: AUSWEICHEN AUF SONSTIGE RECHTSGRUNDLAGEN

- Problem: Herausforderung, umfassend, aber zugleich in einer für den Betroffenen verständlichen Weise zu informieren; andernfalls Einwilligung unwirksam (Art. 7 Abs. 2 S. 2 DSGVO); zudem gemäß Art. 7 Abs. 3 DSGVO stets frei widerrufbar
- Einwilligung ist nach dem Gesetz weder die vorzugswürdige noch die einzige mögliche Rechtsgrundlage
- Verantwortliche also grundsätzlich erst einmal frei, ob er eine Einwilligung einholen, oder die Verarbeitung personenbezogener Daten auf eine sonstige Rechtsgrundlage aus Art. 6 DSGVO stützen will

Zweckänderung und Kumulation von Rechtsgrundlagen

ANTWORTEN DER DSGVO: ZWECKÄNDERUNG UND KUMULATION VON RECHTSGRUNDLAGEN

- Wortlaut von Art. 6 Abs. 1 DSGVO: Deutet darauf hin, dass Rechtsgrundlagen in Art. 6 Abs. 1 nicht nur gleichrangig zueinander sind, sondern **auch gleichzeitig nebeneinander verwirklicht** werden können
- Urteil des EuGH in der Rechtssache Fashion-ID: Ein aus Sicht des Betroffenen einheitlicher Verarbeitungsvorgang kann zugleich auf mehrere Rechtsgrundlagen gestützt werden
- Transparenz! Information!

Risikobasierter Ansatz

ANTWORTEN DER DSGVO: RISIKOBASIERTER ANSATZ

- Risikobasierter Ansatz: Art und Intensität der erforderlichen Maßnahmen abhängig vom Risiko für die Rechte und Freiheiten der betroffenen Personen
  - *Datenschutz durch Technikgestaltung: privacy by design und privacy by default*
  - *Nutzung pseudonymisierter Daten*
  - *Einsatz DSGVO-konformer Datenspeicheroptionen*
- Aus verfahrensrechtlicher Sicht: Konsultationen, Erarbeitung von Verhaltensregeln und Prüfverfahren der Kommission
- Risikobasierter Ansatz für eine innovationsoffene Gesamtbetrachtung notwendig: Sicherung der Chancen und Einflussmöglichkeiten Europas im Zukunftsmarkt

4. Antworten der Praxis

ANTWORTEN DER PRAXIS

- „Privacy paradox“: Betroffene schätzen den Schutz ihrer personenbezogenen Daten und ihrer Privatsphäre in der Theorie hoch, unternehmen aber tatsächlich wenig, um die eigenen Daten aktiv zu schützen und geben diese häufig leichtfertig und freiwillig preis.
- Gründe nicht abschließend geklärt:
  - *Können Betroffene die langfristigen Risiken ihrer Zustimmung nur schwer bewerten bzw. wissen, ob und in welchem Umfang ihre Daten tatsächlich verarbeitet werden?*
  - *Scheu vor dem Aufwand, sich mit datenschutzrechtlichen Risiken für die eigene Privatsphäre ernsthaft auseinanderzusetzen?*
  - *Unkenntnis darüber, welche datenschutzfreundlichen Alternativen bestehen?*

ANTWORTEN DER PRAXIS: SELBSTDATENSCHUTZ

- Datenmanagementsysteme:
  - *Anwendungen zur vereinfachten Einwilligungsverwaltung, wie z.B. Dashboards, aber auch KI-Tools, die individuelle Nutzerpräferenzen automatisch umsetzen (sog. Datenagenten)*
  - *Personal Information Management-Systeme (kurz „PIMS“)*
- Datentreuhandsysteme:
  - *Teilweise oder vollständige Fremdverwaltung der Daten der Nutzer*
  - *Grundgedanke: Systeme haben kein über die Verwaltung hinausgehendes Eigeninteresse an den Daten und können neutral und professionell agieren*
- Ziel: Befähigung des Einzelnen, seine personenbezogenen Daten zu kontrollieren und die Entlastung von Entscheidungen, die ihn überfordern

5. Fazit

FAZIT

Anforderung	Herausforderung	Antwort
Informiertheit und Freiwilligkeit	Überforderungsgrad Soziale Dimension der Entscheidungen	Transparenz Treu und Glauben Privacy by Default DSFA PIMS
Nachweisbarkeit	Verantwortlichkeitsgefüge (Dark Patterns) Betroffenenstruktur	Gemeinsame Verantwortlichkeit Privacy by Design Kumulation von Rechtsgrundlagen
Zweckbindung	Zeitpunkt (Big Data, Machine Learning)	Zweckänderung und Kompatibilitätsprüfung
Widerruflichkeit	Löschpflichten, Nachberichtspflichten	Ausweichen auf oder Kumulation mit anderen Rechtsgrundlagen PIMS

Risikobasierter Ansatz und Verfahren

HÄRTING

Frederike Kollmar, MLE
Rechtsanwältin
kollmar@haerting.de

Maya El-Auwad
Rechtsanwältin
elauwad@haerting.de

HÄRTING Rechtsanwälte | www.haerting.de
Chausseestraße 13, 10115 Berlin | Tel. +49 30 28 30 57 40 | Fax. +49 30 28 30 57 44