Datenschutzerklärungen im Internet
Ergebnisse einer Sichtung

Dr. Jürgen Peemöller

Hamburg, 13. Juni 2019

DR. PEEMÖLLER GESELLSCHAFT
FÜR IT-RISIKO-MANAGEMENT MBH

Agenda

- Informationspflichten
- Vorgehen bei der Sichtung
- Sichtungsfunde
- Fazit

Informationspflichten
(Orientierung am Muster in der GDD-Praxishilfe VII)

1. Datenverarbeiter
    1. Name und Ort des Links
    2. Verantwortlicher und Vertreter (Art. 13, Abs. 1 Buchst. a)
    3. Datenschutzbeauftragter (Art. 13, Abs. 1 Buchst. b)
2. Verarbeitungsrahmen
    1. Zwecke (Art. 13, Abs. 1 Buchst. c)
    2. Struktur der DSE
    3. Rechtsgrundlagen (Art. 13, Abs. 1 Buchst. c)
    4. Berechtigte Interessen (Art. 13, Abs. 1 Buchst. d)
    5. Datenkategorien (Art. 14, Abs. 1 Buchst. d)
    6. Datenquellen (Art. 14, Abs. 2 Buchst. f)
    7. Speicherdauer (Art. 13, Abs. 2 Buchst. a)
    8. Pflicht zur Bereitstellung (Art. 13, Abs. 2 Buchst. e)
    9. Automatisierte Entscheidungsfindung (Art. 13, Abs. 2 Buchst. f)

Informationspflichten
(Orientierung am Muster in der GDD-Praxishilfe VII)

3. Weitergabe und Auslandsbezug
    1. Empfänger oder Kategorien von Empfängern (Art. 13, Abs. 1 Buchst. e)
    2. Drittstaatstransfer (Art. 13, Abs. 1 Buchst. f)
4. Betroffenenrechte
    1. Auskunftsanspruch (Art. 15); Berichtigung (Art. 16); Löschung (Art. 17 Abs. 1); Einschränkung der Verarbeitung (Art. 18); Widerspruch (Art. 21); Datenübertragbarkeit (Art. 20)
    2. Widerruf der Einwilligung (Art. 13, Abs. 2 Buchst. c)
    3. Beschwerderecht (Art. 13, Abs. 2 Buchst. d)

Vorgehen bei der Sichtung

10 Unternehmen (3 DAX, 1 DE Baumarkt, 1 DE Lebensmittelhandel, 1 EU Automobile, 1 EU Versandhandel, 1 DE Telco, 2 DE Legal Firms)

1. Datenverarbeiter
Name und Ort des Links

Meist

- Datenschutzerklärung

aber auch

- Datenschutzerklärung und Datenschutzinformation
- Datenschutzhinweise
- Privacy (Datenschutz)

Verweis immer in Fußzeile oder -bereich

2. Verantwortlicher und Vertreter

Ja, aber manchmal

- Verweis auf Impressum
  - nur indirekt über „Contact Us“
- Liste von Firmen (wer ist für was verantwortlich?)
- Liste von Firmen, abhängig von der Art der Verarbeitung

Postadresse, manchmal zusätzlich

- Liste von Namen von Vorständen/Geschäftsführern (bei Verweis auf Impressum)
- Email-Adresse (datenschutz@, impressum@, kundenmanagement, Kunden Log-In)

3. Datenschutzbeauftragter

Ja, immer

- Fast immer funktionale Email-Adresse, einmal Name und Postadresse
- Manchmal zusätzlich Postadresse und Telefon

2. Verarbeitungsrahmen
1. Zwecke

Meistens Website spezifisch (-> Kunden und Interessenten)

- Besuch der Website (Abruf von Informationen, angebotene Leistungen in Anspruch nehmen)
- Kontaktaufnahme (E-Mail, Kontaktformular)
- Anfordern von Informationen
- Bestellen Newsletter
- Services/Dienstleistungen: „um Produkte und Dienstleistungen bereitzustellen und kontinuierlich zu verbessern“
- Webanalyse mit Google Analytics,
- Newsletter
- Abgleich Embargolisten

Selten unabhängig von der Website, z.B.

- Mandant
- Veranstaltungsbesucher
- Lieferant
- Dienstleister
- Besucher
- auf Videoüberwachung
- Bewerber
- Mitarbeiter

2. Struktur der Datenschutzerklärung

Sehr unterschiedlich

- direkt an DSGVO orientiert,
- sehr aus Nutzersicht („Wir und Du“)

Manchmal

- Allgemeines vorab
- und dann spezifisch pro Verarbeitung oder Zielgruppe
- Auch Russland-spezifischer Hinweis
  „ (…) dass Sie sich ausdrücklich damit einverstanden erklären, dass XXX Ihre personenbezogenen Daten erfassen darf und diese Daten in den USA und in anderen Ländern verarbeitet und dass Sie XXX nicht für eine etwaige Nichteinhaltung von Gesetzen der Russischen Föderation verantwortlich machen.

3. Rechtsgrundlagen

Sehr unterschiedlich

- Mal kurz an DSGVO orientiert (ggf. im spezifischen Teil detaillierter):
  - Bei ausdrücklicher Einwilligung: Art. 6 Abs. 1a
  - Bei vorvertraglichen Maßnahmen: Art. 6 Abs. 1b
  - In allen anderen Fällen: Art. 6 Abs. 1f (und Hinweis auf Widerspruchsrecht)
- Mal implizit oder sehr pauschal
  - „Schließen Sie einen Mobilfunk-Vertrag bei uns ab, nutzen wir Ihre Kundendaten in erster Linie, damit wir den Vertrag mit Ihnen erfüllen können, um z. B. Ihre Telefonate durchzuführen, Ihnen die Webseiten anzuzeigen, die Sie ansurfen oder die bei Ihrem XXX-Pass inkludierten Apps zu identifizieren und die verbrauchten Daten richtig abzurechnen. Dafür verwenden wir Ihre Mobilfunknummer und die Web-Adresse, unter der Sie die App abrufen.“
  - "innerhalb des geltenden Rechts"
- Mal nur für spezifische Verarbeitungen bzw. Übermittlungen
  - Bonitätsprüfungen (berechtigtes Interesse) (s.u.)

4. Berechtigte Interessen

- Allgemeines Motto: Wir wollen Sie effektiv (zielgerichtet) und effizient (Kosten und Zeit) bedienen.
- „Die Erhaltung der Funktionsfähigkeit unserer IT-Systeme, aber auch die Vermarktung eigener und fremder Produkte und Dienstleistungen und die rechtlich gebotene Dokumentation von Geschäftskontakten sind solche berechtigten Interessen.“
- „Wir übermitteln im Rahmen dieses Vertragsverhältnisses erhobene personenbezogene Daten über die Beantragung, die Durchführung und Beendigung dieser Geschäftsbeziehung sowie Daten über nicht vertragsgemäßes Verhalten oder betrügerisches Verhalten an die SCHUFA Holding AG, Kormoranweg 5, 65201 Wiesbaden. Rechtsgrundlagen dieser Übermittlungen sind Artikel 6 Absatz 1 Buchstabe b und Artikel 6 Absatz 1 Buchstabe f der Datenschutz-Grundverordnung (DS-GVO). Übermittlungen auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DS-GVO dürfen nur erfolgen, soweit dies zur Wahrung berechtigter Interessen der XXX1 GmbH sowie der XXX2 GmbH oder Dritter erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Der Datenaustausch mit der SCHUFA dient auch der Erfüllung gesetzlicher Pflichten zur Durchführung von Kreditwürdigkeitsprüfungen von Kunden (§ 505a und 506 des Bürgerlichen Gesetzbuches).“

5. Datenkategorien

Obwohl bei Erhebung nicht erforderlich

- Meist detaillierte Auflistung pro Zweck, Verarbeitung, Service, Produkt
- Insb. bei Google Analytics o. dgl.
- Auch ggf. Unterscheidung
  - „Informationen, die Sie uns geben“
  - Automatische Informationen
  - Informationen aus anderen Quellen
- Allerdings meist beispielhaft:

  „Durch diese Handlungen können Sie uns folgende Informationen zur Verfügung stellen: Ihr Name; Adresse und Telefonnummer; Zahlungsinformationen; Ihr Alter; Ihre Standortinformationen; Personen, an die Einkäufe versendet wurden oder Personen, die in 1-Click-Einstellungen aufgeführt sind (einschließlich Adressen und Telefonnummern); **E-Mail-Adressen Ihrer Freunde und anderer Personen***; Inhalte von Bewertungen und E-Mails an uns; persönliche Beschreibung und Foto in Ihrem Profil; Sprachaufzeichnungen, wenn Sie mit Alexa sprechen; Bilder und Videos, die im Zusammenhang mit Amazon Services gespeichert sind; Informationen und Dokumente bezüglich Identität und Stand; Unternehmens- und Finanzinformationen; Informationen bezüglich Ihrer Kreditgeschichte; MwSt-Nummern; und Geräteprotokolldateien und -konfigurationen, **einschließlich W-Lan-Anmeldedaten, wenn Sie diese automatisch mit Ihren anderen Amazon-Geräten synchronisieren lassen***.“

  *Fette Hervorhebung vom Referenten

6. Datenquellen

Bei Erhebung ebenfalls nicht erforderlich

- Selten, da wohl häufig keine Verwendung aus anderen Quellen

Beispiel für beispielhafte Aufzählung (Mix von was, wie und von wem):

- Aktualisierte Informationen über Bestell- und Lieferadresse von unseren Paketzustellern und anderen Transportunternehmen, die wir dazu verwenden, unsere Datenbank zu aktualisieren, um Ihre nächsten Bestellungen sicher stellen zu können und zu gewährleisten, dass wir mit Ihnen einfacher kommunizieren können;
- Informationen über Konten, Kauf - und Zahlungsverhalten, Page View Informationen, oder andere Informationen über Ihre Interaktionen mit Geschäften, mit denen wir gemeinsam (co-branded) Angebote unterhalten oder für die wir technische, Erfüllungs-, Zahlungs-, Werbe- oder andere Dienstleistungen anbieten;
- Informationen über Ihre Interaktionen mit Produkten und Dienstleistungen unserer Tochtergesellschaften;
- Suchergebnisse und Links, einschließlich bezahlter Listungen;
- Informationen über mit dem Internet verbundene Geräte und Dienste, die Sie mit Alexa verbunden haben; und
- Auskünfte bezüglich der Kreditgeschichte von Kreditauskunfteien, die wir dazu verwenden, Missbrauch, insbesondere Betrug, zu verhindern und aufzudecken und dazu, bestimmten Kunden bestimmte Finanzdienstleistungen und Zahlungsarten anbieten zu können.

7. Speicherdauer

- Pauschale Regel:
  Solange wie für den Zweck oder von Gesetz o. dgl. erforderlich
- Teilweise auch genaue Fristen

8. Pflicht zur Bereitstellung
9. Automatisierte Entscheidungsfindung

Pflicht zur Bereitstellung ist in der DSE häufig nicht direkt angesprochen. Nur die Konsequenz:

- Wenn keine Daten, dann keine oder nur eingeschränkte Leistung möglich
  (ggf. Unterscheidung Muss- und Kann-Daten)

Automatisierte Entscheidungsfindung

- Bei Schufa etc. erwähnt (zugehörige DS-Info beigefügt)
- Profiling: „So analysieren wir Ihre Daten mithilfe von mathematisch-statistischen Verfahren, um Werbung auf Ihre individuellen Interessen zuschneiden zu können.“

3. Weitergabe und Auslandsbezug
1. Empfänger oder Kategorien von Empfängern

Unterschiedliche Detaillierung (meist Kategorien, selten konkrete Empfänger)

- IT-Dienstleister, Google und dessen Partnerunternehmen
- Detaillierte Listen von Kategorien
- "Partner", zB Kundenservice oder RZ; deutsche Behörden bei rechtl. Verpflichtung:
  „Sie und der Gesetzgeber entscheiden, wie wir mit Ihren Daten umgehen. Haben Sie uns keine gesonderte Einwilligung erteilt, geben wir Ihre persönlichen Daten nur weiter, wenn wir das nach deutschem oder europäischem Recht dürfen oder müssen. Mit einigen Partnern arbeiten wir besonders eng zusammen, z.B. im Kundenservice oder mit Rechenzentren. Damit diese Partner Ihre persönlichen Daten in unserem Auftrag verarbeiten dürfen, machen wir detaillierte vertragliche Vorgaben.“
- Amazon-Töchter, aber auch Dritt-DL zur Erfüllung von Aufgaben „für uns“ UND wenn AGB und Vereinbarungen durchzusetzen sind, Schutz der Interessen von amazon/Dritter, ua Mißbrauch und Kreditkartenbetrug

2. Drittstaatstransfer

Sehr unterschiedlich

- Nein
- Nein bis auf Google (Irland, USA wegen Privacy Shield)
- Ja, aber Daten nur in D; AV haben nur Einsicht und Bearbeitung; außerhalb EU nur mit EU-Standardvertragsklauseln oder Kommissions-beschluß
- Ja oder ggf. (mit Verweis auf EU-Standardvertragsklauseln; einmal Hinweis, dass bei der Vorlage von Kopien von Garantien ggf. überwiegende Rechte Dritter oder gesetzliche oder vertragliche Geheimhaltungspflichten zu berücksichtigen sind)
- Ja in Übereinstimmung mit DSE und anwendbaren DS-Gesetzen; Verweis auf Extra-Seite zum Privacyshield: TRUSTe, …. und ggf. nationale Sicherheitsinteressen

4. Betroffenenrechte

1. Auskunftsanspruch (Art. 15); Berichtigung (Art. 16); Löschung (Art. 17 Abs. 1); Einschränkung der Verarbeitung (Art. 18); Widerspruch (Art. 21); Datenübertragbarkeit (Art. 20)
   - Meist kurze oder längere Auflistung

2. Widerruf der Einwilligung
   - Ja (bis auf einmal; dort vermutlich bei der Einwilligung)

3. Beschwerderecht
   - Hinweis vorhanden
     - Meist mit Angabe der Aufsichtsbehörde(n)
     - Manchmal auch nur abstrakt

Fazit

- Meist nur auf Webseiten-Besucher und Kunden zugeschnitten
- Andere Gruppen eher selten
  (aber empfehlenswert; insb. für Mitarbeiter von Geschäftspartnern wg. Visitenkartenproblem!)
- Gewisser Überblick für den interessierten Laien möglich
- Prüfung auf „Hintertüren“ auch für Fachmann manchmal schwierig wegen beispielhafter Angaben und unterschiedlicher Strukturen

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Peemöller Gesellschaft
für IT-Risiko-Management mbH