Die DSGVO – Ein Update aus der Sicht eines Datenschutzbeauftragten

Roman Maczkowsky
Geschäftsführer m-privacy GmbH
r.maczkowsky@m-privacy.de oder
datenschutz@eprd.de

m-privacy GmbH
Werner-Voß-Damm 62
12101 Berlin

www.m-privacy.de

Leitbild der DSGVO - Transparenz und Verantwortung

- DSGVO fordert Management der Verarbeitung personenbezogener Daten
- Inklusive Nachweispflicht Art. 5 Nr. 2 DSGVO
- Transparenzpflichten nach Artt. 13, 14 DSGVO
- Verfahrenzverzeichnis Art. 30 DSGVO

Management der Verarbeitung

Die DSGVO fordert nicht weniger als ein Datenschutz-Management

- Alle Verarbeitungstätigkeiten pb-Daten müssen erfasst sein → Erfassungsbogen Bereichsleitende
- Zu allen Verarbeitungen müssen schriftliche Arbeitsanweisungen hinterlegt sein
- Mit Dienstleistern: Auftragsverarbeitungs-Vertrag → AVV

Wieviele Verfahren haben Sie erfasst?

Nr.	Wie heißt das Verfahren? Name des Verfahrens	Wer ist verantwortlich? (Möglichst nur eine oder zwei Personen benennen). [Alternativ: zuständige Funktion + Ansprechperson]	Welchen Zweck hat die Daten-verarbeitung?	Welche personenbezogenen Daten werden verarbeitet (Z.B. Kontaktdaten, Kontodaten, Buchungspräferenzen, Daten aus der Online-Nutzung)?	Wessen Daten werden verarbeitet (Z.B. Mitarbeitende Büro Berlin, Interessenten aus dem Internet)?

Transparenzpflichten Artt. 13, 14 DSGVO

Transparenz- und Informationspflichten erfordern

- Bei Erhebung: Angaben zum Zweck und zu Widerspruchsoptionen → Erhebungs-Disclaimer
- Bei jeder Nutzung: Informationen zur verantwortlichen Organisation, dem Zweck, der Rechtsgrundlage und dem Widerspruchsrecht mitzusenden → Nutzungs-Disclaimer
- Bei Erhebung bei Dritten (Bsp. Presseverteiler) zudem auf die Quelle hinweisen. (Art. 14 DSGVO)
- Die zu verwendenden Disclaimer sind in der AA, im internen Datenschutzblatt oder in der Liste der Verarbeitungstätigkeiten (VVZ) zu hinterlegen

Disclaimer-Beispiel

für Presseverteiler (Journalisten)

- Wir nehmen den Schutz Ihrer personenbezogenen Daten sehr ernst. Verantwortlich für die Datenerhebung ist der BDN e.V., Berlin.
- Wir verarbeiten Ihre Daten zum Zweck der Übermittlung von Presseinformationen gemäß Art. 6 Abs. 1 lit. f DSGVO. Ursprung der Daten sind eigene Recherchen aus öffentlich zugänglichen Quellen oder persönliche Kontakte.

- Weitere Informationen zum Datenschutz finden Sie in unseren Datenschutzhinweisen (https://BEISPIEL.com/de/pages/rechtliche-hinweise/agb-und-datenschutz).

Schutz personenbezogener Daten

- Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen.

Grundsatz:

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der oder die Betroffene zugestimmt hat.

Das Prinzip: Verbot mit Erlaubnisvorbehalt

Grundsatz:
(Art. 6, Abs. 1 DSGVO)

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden **Bedingungen erfüllt** ist:

a) Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere **bestimmte Zwecke** gegeben;

b) die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich [...]

f) die Verarbeitung ist zur Wahrung der **berechtigten Interessen** des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen [...] der betroffenen Person [...] überwiegen [...].

Gute Praxis des Datenschutzes

Vor Erhebung, Nutzung oder Verarbeitung personenbezogener Daten:

- Umfassende Aufklärung
- Eindeutige Zweckbindung
- Einholung der Zustimmung
  auf Basis übermittelter Information

Analogie:
Patientengespräch im Vorfeld medizinischer Therapie mit dem Ziel einer informierten Einwilligung nach Aufklärung („Informed Consent“).

Newsletter mit Double-Opt-In (DOI)

- Der Newsletter basiert auf der Einwilligung der Betroffenen nach Art. 6, Abs. 1 lit. a)
- Nach dem Eintrag über die Website erhalten die Nutzer eine Verifikations-E-Mail
- Erst nach Aufruf des darin enthaltenen Links ist die Anmeldung bestätigt.

Auch wenn die DSGVO nur ein einfaches Opt-In vorschreibt, wird bei Newslettern das DOI-Verfahren zwecks Nachweisbarkeit empfohlen.

Nicht jede Verarbeitung …
basiert auf einer Einwilligung

Datenschutzhinweise auf der Website

Selbsttest:

Welche Dienste sind eingebunden?

webbkoll.dataskydd.net

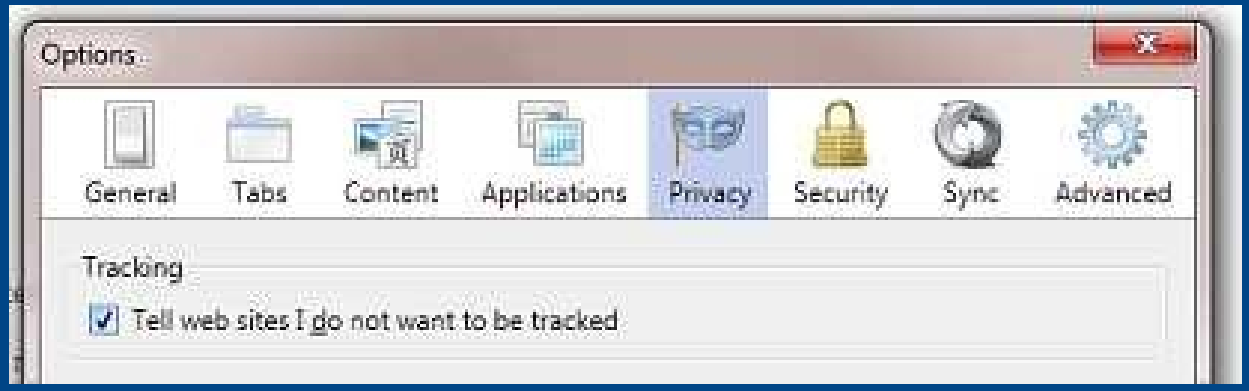
Datenschutzhinweise enthalten

- Nennung der Verarbeitungszwecke
- Angaben zum DSB
- Transparenzangaben zu Cookies, Trackern und eingebundenen Diensten
  → vgl. Webbkoll-Test
- Hinweise auf Widerspruchsmöglichkeiten
  → DNT berücksichtigen
- Nennung der Betroffenenrechte
- Versionierung

Do Not Track

Dem uneingewilligten Tracking widersprechen

- Die „nicht-verfolgen“-Option im Browser



- Faire Datenschutzpolicy für Besucher
- Respektiert den mittels Browsereinstellung (DNT) geäußerten Wunsch nicht uneingewilligt getrackt zu werden.
- Widerspruch im Sinne von § 15 Abs. 3 TMG / Art. 21 DSGVO
  www.datenschutz-berlin.de/attachments/861/JB_11_Inhalt_Web.pdf

DNT-Merkmal als Opt-Out

Do not Track

Zur Verbesserung unseres Online-Angebotes erheben wir statistische Daten über Ihren Besuch dieser Website. Die von uns eingesetzten Tracking-Maßnahmen werden auf Grundlage des Art. 6 Abs. 1 lit. f) DSGVO zur Wahrung unserer berechtigten Interessen an einer fortlaufenden Optimierung dieser Internetpräsenz durchgeführt.

Gemäß § 15 (3) Telemediengesetz beziehungsweise Art. 21 DSGVO haben Sie das Recht, dagegen Widerspruch einzulegen. Wenn Sie in unsere statistische Erfassung nicht einbezogen werden möchten, können Sie in Ihrem Browser das Merkmal "Do not Track" aktivieren. Wir interpretieren das so von Ihnen gesetzte Merkmal als Wunsch, nicht ungefragt "getrackt" zu werden. Dementsprechend wird dieses Merkmal bei allen Besuchen unserer Website ausgewertet und jegliche Trackingmaßnahmen entfallen. Dies gewährleistet bestmöglichen Datenschutz, ohne dass Sie weitergehende Maßnahmen im Hinblick auf unsere Website ergreifen müssten.

Beispiel von der Website

Datenschutzerklärung

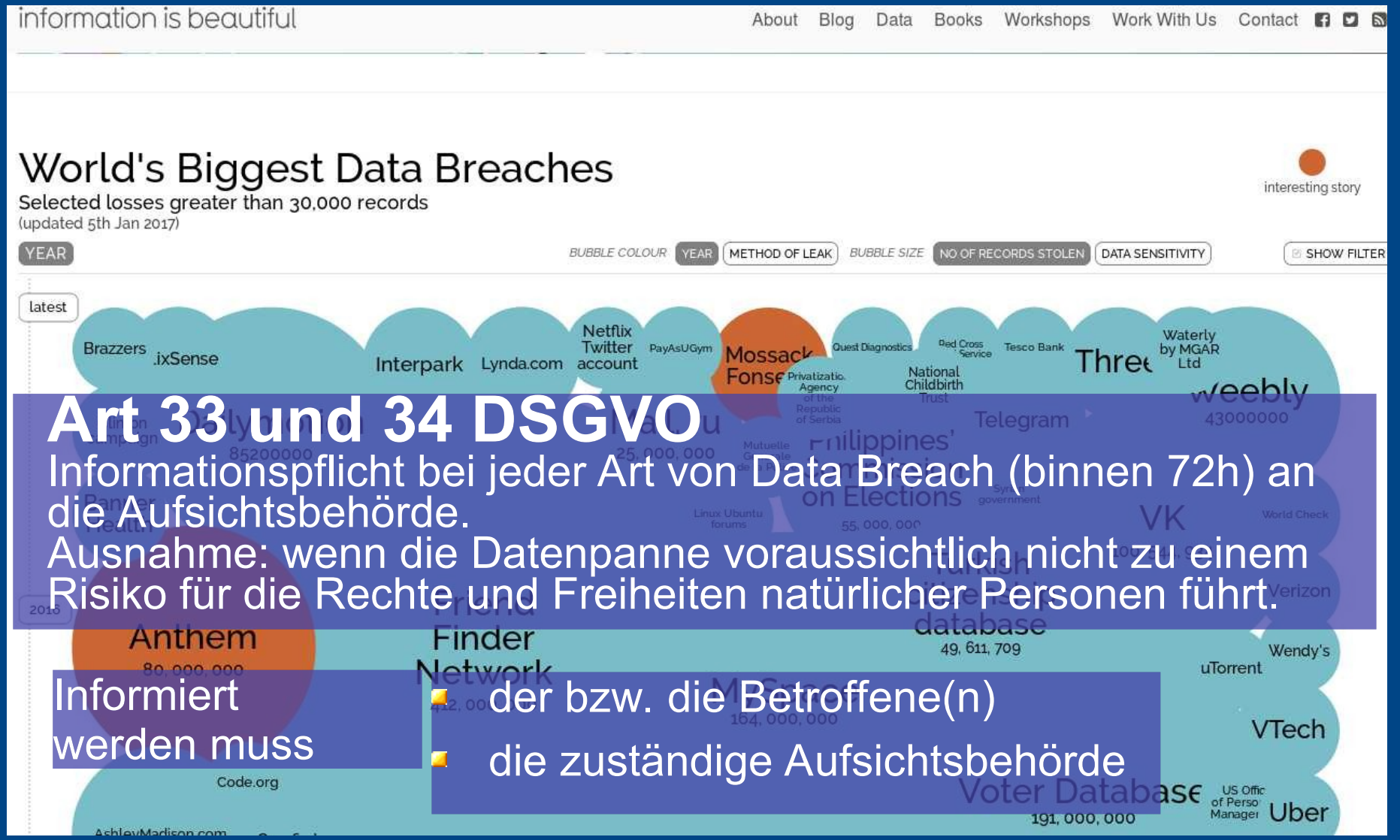
3. Respektierung von 'Do not Track'

Wir respektieren selbstverständlich „Do not track“ (DNT)

Wir weisen darauf hin, dass generelles Abschalten von Cookies Funktionsstörungen bei der Benutzung unserer Internetpräsenz hervorrufen kann und überdies eine Datenübermittlung an Google Analytics nicht zuverlässig ausschließt. Wir empfehlen daher, die „Do not track“-Option (DNT) Ihres Internetbrowsers zu nutzen. Es handelt sich je nach Browser entweder um einen Schalter in den Programmeinstellungen. Wird diese Option aktiviert, signalisiert Ihr Browser unserem Webserver, dass Sie keine Tracking-Maßnahmen ohne Ihre explizite Einwilligung wünschen. Daraufhin werden unsererseits automatisch sämtliche Tracking-Funktionen serverseitig deaktiviert. Dies bedeutet auch, dass unsere Webseiten ohne Code für Google Analytics ausgeliefert werden. Dies gewährleistet bestmöglichen Datenschutz, ohne dass Sie weitergehende Maßnahmen im Hinblick auf unsere Internetpräsenz ergreifen müssten.

https://www.aerzte-ohne-grenzen.de/datenschutz-und-datensicherheit

Data Breaches – informationisbeautiful.net



Art 33 und 34 DSGVO

Informationspflicht bei jeder Art von Data Breach (binnen 72h) an die Aufsichtsbehörde.

Ausnahme: wenn die Datenpanne voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Informiert werden muss

- der bzw. die Betroffene(n)
- die zuständige Aufsichtsbehörde

Vielen Dank!

Ich freue mich auf Ihre Fragen.

Roman Maczkowsky
Externer Datenschutzbeauftragter der LucaNet AG
datenschutz@lucanet.com

m-privacy GmbH
Werner-Voß-Damm 62
12101 Berlin

www.m-privacy.de

2018-09-29