

Datensalat leicht verdaulich

Datenschutz nach DSGVO für kleine NGOs

Programm

- Vorstellungsrunde, Stand der Dinge
- Überblick DSGVO
- Pause
- Fragen

Grundlagen

- Historie Datenschutz (Eid des Hippokrates 400 v.C., Giro Regelement 18. JH)
- Verfassung und EU (BverfG, GR Charta)
- DSGVO - Verbraucherschutz - einheitlicher Markt

DSGVO

- Ziele - Binnenmarkt, Verbraucherschutz, GR Schutz
- Neu/Alt? (Sanktionen, Einwilligung, Informationspflicht!, Grundsätze, EU, Vergessenwerden, Portabilität, Meldepflicht)
- Thema: „Verarbeitung personenbezogener Daten“

Personenbezogene Daten

... alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

Verarbeiten

- ... jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das **Erheben**, das **Erfassen**, die **Organisation**, das **Ordnen**, die **Speicherung**, die **Anpassung** oder **Veränderung**, das **Auslesen**, das Abfragen, die **Verwendung**, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das **Löschen** oder die Vernichtung;

Grundsätze für die Verarbeitung personenbezogener Daten, Art. 5

- Rechtmäßigkeit, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

Rechtmäßigkeit, Art. 6

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

1. Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
2. die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
3. die Verarbeitung ist zur Erfüllung einer **rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;
4. die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen;
5. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im **öffentlichen Interesse** liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
6. die Verarbeitung ist zur Wahrung der **berechtigten Interessen des Verantwortlichen** oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Informationspflichten bei der Erhebung personenbezogener Daten

- Transparenzgrundsatz
- Katalog in Art. 13/14
- Medienbruch erlaubt

Verzeichnis von Verarbeitungstätigkeiten, Art. 30

- Pflicht?
- nicht öffentlich (Qualitätskontrolle, Aufsicht), schriftlich, aktualisieren
- Inhalt: (gleich); Muster (S. 14)
- BaFin vs. BMVert

Inhalt

Verarbeitungsverzeichnis

- Name, Kontakt Verantwortlicher
- Zweck der Verarbeitung
- Kategorien der Daten
- Empfänger? Drittstaaten?
- ggf. Löschfristen
- konkrete Verarbeitungstätigkeit (speichern, erheben ...)
- herangezogene Rechtsgrundlage

Auftragsverarbeitung

- z.B. Mitarbeiterdaten an ext. Buchhaltung
- z.B. Wartung der IT-Systeme durch Externe
- Privilegierung: keine Einwilligung nötig
- Aber: weisungsabhängig! (nicht RA und StB)
- Auswahl des AV: Haftung für diesen
- Vertrag: z.B. Daten löschen
- Kontrollrechte
- Ende des AVV

Sicherheit der Verarbeitung

- IT-Sicherheit (z.B. Passwörter)
- Berechtigungsmanagement
- Risiken bestimmen und begegnen
- Verschlüsselung, Aktualisierung
- E-Mail Kommunikation cc, bcc

Datenschutzbeauftragter

- Organ der Selbstkontrolle
- unter bestimmten Bedingungen Pflicht, auch freiwillig
- Aufgaben (Beratung, Überwachung, Zusammenarbeit mit Behörden etc.)

Betroffenenrechte

- Transparente Information („präziser, transparenter, verständlicher und leicht zugänglicher Form in einfacher und klarer Sprache“)
- Auskunft
- Berechtigung, Löschung, Einschränkung der Verarbeitung
- Datenübertragbarkeit
- Widerspruch gegen die Verarbeitung (jederzeit)

Verletzung des Schutzes personenbezogener Daten

- Art. 33, 34
- Meldung an die Aufsichtsbehörde
- Benachrichtigung der Betroffenen
- Rat durch Fachleute

Sanktionen und Haftung

- Geldbußen (wirksam, verhältnismäßig, abschreckend)
- Schadensersatz (materiell und immateriell)
- Art. 82, 83

Vereinsstruktur

- Verantwortlichkeit
- Datenschutzgrundsätze – Datenschutzkonzept (1/2 Seite)
- Betroffenenrechte
- Technik!
- Auftragsverarbeitung?
- Verzeichnis der Verarbeitungstätigkeiten
- Meldungen an Aufsicht/Betroffene

Aufsichtsbehörden

- Anspruch auf Beratung
- personell aufgestockt
- Risiken?

Fotos

- Fotos von Mitarbeitern
- Einwilligungserklärung? (Muster)
- Minderjährige

Pause

Recap

- Grundsätze
- Rechtmäßigkeit (Einwilligung, Vertrag, berechtigtes Interesse)
- Verarbeitungsverzeichnis, Datenschutzkonzept
- IT Sicherheit
- Verhältnismäßigkeit!

Grundsätze für die Verarbeitung personenbezogener Daten, Art. 5

- Rechtmäßigkeit, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

Fragen

- Fragensammlung BER
- und alle anderen Fragen

Vielen Dank

Jan Kalbhenn, Rechtsanwalt

www.ra-kalbhenn.com

jk@ra-kalbhenn.com