

Fluch oder Segen

–

Der richtige Umgang mit der
Datenschutzgrundverordnung DSGVO

Stephan Zieger

Bundesverband Freier Tankstellen

Spielverderber Datenschutz?

Datenschutzgrundverordnung

- unmittelbar geltendes Gesetz
- 99 Artikel
- 173 Erwägungsgründe

Datenschutzgrundverordnung

- gilt für Jeden
- automatisierte Datenverarbeitung
- nicht automatisierte Datenverarbeitung
- auch schon für „Vorbereitungshandlungen“

Datenschutzgrundverordnung

Artikel 4 Abs. 1 DSGVO sagt:

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

„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;*

Datenverarbeitung

Artikel 4 Abs. 2 DSGVO sagt:

Im Sinne dieser Verordnung bezeichnet der Ausdruck: (...)

„Verarbeitung“ 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**;

Umgang mit Daten

Zweckbindung

Werden Daten für einen bestimmten Zweck verarbeitet, dann dürfen die Daten auch nur für diesen Zweck verwendet werden. Daten die zum Beispiel für die Erfüllung eines Vertrages gespeichert werden, dürfen auch nur für diesen Vertrag genutzt werden.

Die Nutzung der Daten für einen anderen Zweck sind verboten

Umgang mit Daten

Direkterhebung

Datenschutzrechtlich gibt es den Vorrang der Direkterhebung. Daten sollten grundsätzlich direkt beim Betroffenen erhoben werden.

Wenn Daten nicht beim Betroffenen selbst erhoben werden Art. 13 und 14 beachten (Informationspflichten gegenüber dem Betroffenen).

Umgang mit Daten

Transparenz

Die betroffene Person soll jederzeit wissen, wer welche Daten über sie speichert. Dies bedeutet, dass Daten nicht ohne weiteres weitergegeben werden dürfen.

Umgang mit Daten

Erforderlichkeit

Der Grundsatz der Erforderlichkeit besagt, dass die Datenverarbeitung sich auf den geringst möglichen Eingriff beschränken muss. Die Verarbeitung von Daten muss sich auf das für die jeweilige Zweckerreichung notwendige Maß beschränken. Eine reine Ausforschung ist nicht zulässig.

Umgang mit Daten

Datenvermeidung und Datensparsamkeit

Bei der Gestaltung und Auswahl von Datenverarbeitungssystemen ist das Ziel zu beachten, keine oder so wenige personenbezogenen Daten wie möglich zu verarbeiten. **Nach Möglichkeit sollen Daten anonymisiert oder pseudonymisiert werden.**

Einwilligung

Daten dürfen nur mit Einwilligung des/ der Betroffenen erhoben werden (Art. 7 und 8)

- Grundsatz: Die Verarbeitung von personenbezogenen Daten ist nur dann zulässig, wenn der Betroffene entsprechend eingewilligt hat oder eine gesetzliche Norm die Verarbeitung erlaubt.
- Häufigste Erlaubnisnorm: Die Verarbeitung ist für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen.

Einwilligung

- Der Verarbeiter muss nachweisen können, dass eine Einwilligung
- Vorformulierte Einwilligungserklärung müssen in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache; klare Absetzung von anderen Sachverhalten (z.B. AGB)
- Über Widerrufsmöglichkeit muss aufgeklärt werden
- Anforderungen an Minderjährigenschutz sind sehr hoch
- Minderjährigkeit im Datenschutz endet mit 16

Danke für Ihre
Aufmerksamkeit?

Datenschutzmanagement

1. Organisation/Verantwortlichkeit
2. Verzeichnis der Verarbeitungstätigkeiten erstellen
3. IT-Sicherheitskonzept/ technische und organisatorische Maßnahmen
4. Datenschutzfolgeabschätzungen durchführen, sofern erforderlich
5. Vertragsmanagement – Verträge mit Auftragsverarbeitern anpassen
6. Mitarbeiterbelehrung und Verpflichtung auf den Datenschutz
7. Informationspflichten
8. Kundeninformation
9. Datenschutzbeauftragter?
10. Prozess zur Meldung von Datenschutzverletzungen erstellen.

Verantwortlicher

- Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Verzeichnis der Verarbeitungstätigkeiten

Rechtsgrundlage: Art. 30 DSGVO

Das **Verarbeitungsverzeichnis** kann schriftlich oder elektronisch erstellt werden und sollte folgende Punkte beinhalten:

Namen und Kontaktdaten des Verantwortlichen und ggf. des Datenschutzbeauftragten

Zweck der Verarbeitung

Kategorien der betroffenen Personen und der personenbezogenen Daten

Kategorien der Datenempfänger

Angaben zu Übermittlungen in ein Drittland

Löschfristen

technische und organisatorische Schutzmaßnahmen

Muster für Verzeichnisse gibt es auf zahlreichen Internetseiten zum [Download](#).

Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten“ gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf abrufbar.



Muster 12: Einzelhändler – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:

Bekleidungshaus Huber
Hinterer Weg 15
91522 Fallstadt

Tel. 0981/123456-0

E-Mail: info@modehuber-fallstadt.de

Web: www.modehuber-fallstadt.de

Inhaber: Gerhard Huber, geb. 21.02.1986

Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbez. Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über Buchhaltungsbüro)	Hans Klausen 0981/123456-1 hans@modehuber-fallstadt.de	01.01.2018	<ul style="list-style-type: none"> Auszahlung der Löhne/Gehälter Abfuhr Sozialabgaben u. Steuern 	Beschäftigte	<ul style="list-style-type: none"> Name und Adressen der Beschäftigten ggf. Religionszugehörigkeit Eindeutige Kennzahlen zur Steuer... 	Buchhaltungsbüro	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Betrieb der Webseite (über Hosting-Dienstleister)	Peter Diercksen 0981/123456-2 peter@modehuber-fallstadt.de	19.03.2018	Unternehmensdarstellung	<ul style="list-style-type: none"> Kunden Webseitenbesucher 	<ul style="list-style-type: none"> IP-Adressen 	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept
Kundenkartenverwaltung	Marie Greiner 0981/123456-3 marie@modehuber-fallstadt.de	19.03.2018	Verwaltung der Kundendaten	Kunden	<ul style="list-style-type: none"> Stammdaten der Kunden Kaufhistorien 	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Zahlungsabwicklung bei Kunden (über externen Dienstleister)	Peter Diercksen 0981/123456-2 peter@modehuber-fallstadt.de	19.03.2018	Durchführung der Zahlungsverarbeitung	Kunden	<ul style="list-style-type: none"> Stammdaten der Kunden Zahlungsdaten (Bankverbindung) 	Zahlungsdienstleister	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Werbemaßnahmen zur Kundengewinnung und -bindung	Marie Greiner 0981/123456-3 marie@modehuber-fallstadt.de	20.03.2018	Marketing zur Kundenakquirierung	<ul style="list-style-type: none"> Bestandskunden potenzielle Neukunden 	<ul style="list-style-type: none"> Postadressen der Kunden 	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
...

Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Automatische Updates im Betriebssystem aktivieren
- ✓ Standard-Gruppenverwaltung (z. B. in Windows)
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Aktueller Virens Scanner/Sicherheitssoftware
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Standard-Shredder

IT-Sicherheitskonzept

Wer Daten verarbeitet braucht ein IT-Sicherheitskonzept. IT-Sicherheitskonzept heißt, **technische und organisatorische Maßnahmen** zum Schutz der Daten und zum Schutz vor Datenverlust

- Pseudonymisierung
- Verschlüsselung (Passwortzugang)
- Gewährleistung der Vertraulichkeit (Zutritt und Zugang)
- Gewährleistung der Integrität
- Daten müssen richtig sein
- Gewährleistung der Verfügbarkeit (Stromausfall/ technische Probleme/ Verfügbarkeit des Systems)
- Schutz gegen Hacker
- Schutz vor Viren
- Wiederherstellung bei Datenverlust
- Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Datenschutzfolgeabschätzung

Art. 35 DSGVO-Datenschutz-Folgenabschätzung

„... Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.“

Das Ergebnis ist zu dokumentieren. Je nach Ergebnis ist ein Datenschutzbeauftragter zu bestellen.

Datenschutzfolgeabschätzung

Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche;

Datenschutzfolgeeinschätzung

Schutzbedarf	Klasse	Erläuterungen Beeinträchtigung des Persönlichkeitsrechts	Beispiele
Normal (Gering oder Mittel)	1	<p>Wäre für Betroffene als tolerabel einzustufen. Ein möglicher Datenmissbrauch hätte nur geringfügige Auswirkungen (wirtschaftlich/gesellschaftspolitisch) für Betroffene.</p> <ul style="list-style-type: none"> - Nicht zur Veröffentlichung bestimmte Daten - Geringfügige Schäden bei Veröffentlichung/Verfälschung 	<p>Gering: Öffentliche Register, Anschrift, Kontaktdaten</p> <p>Mittel: Daten über Geschäfts- und Vertragsbeziehungen, Kontostände, Prüfungsergebnisse, Personaldaten (soweit nicht Stufe 2), Kreditauskünfte</p>
Hoch	2	<p>Wäre für Betroffene als erheblich einzustufen. Ein möglicher Datenmissbrauch hätte erhebliche Auswirkungen (wirtschaftlich/gesellschaftspolitisch, ggf. Beeinträchtigung der persönlichen Unversehrtheit) für Betroffene.</p> <ul style="list-style-type: none"> - Sensible Daten - Hohe Folgeschäden bei Veröffentlichung/Verfälschung 	<p>Steuerdaten, strafbare Handlungen; Daten, die einem Berufs-, Geschäfts-, Fernmelde- oder Mandantengeheimnis unterliegen; Personaldaten (soweit nicht Stufe 1) wie z. B. Beurteilungen, berufliche Laufbahn, Angaben über Behinderung etc.</p>
Sehr hoch	3	<p>Wäre für Betroffene als besonders bedeutsam und als nicht tolerabel einzustufen. Ein möglicher Datenmissbrauch bedeutet für Betroffene wirtschaftlichen/gesellschaftspolitischen Ruin oder beeinträchtigt die persönliche Unversehrtheit gravierend.</p> <ul style="list-style-type: none"> - Hochsensible Daten - Veröffentlichung/Verfälschung verletzt Persönlichkeitsrechte, verursacht Schaden an Leib und Leben oder Ansehender Betroffenen 	<p>Adressen von polizeilichen V-Leuten, Adressen von Zeugen in bestimmten Strafverfahren</p>

Auftragsdatenverarbeitung

Nur als Erinnerungsposten:

- Wer Daten von fremden Anbieter verarbeiten läßt, muß eine entsprechende Vereinbarung abschließen.
- Bsp.: Mailing durch Drittanbieter, Auswertung von Kundenumfragen durch Dritte
- Inhalt ähnlich wie das Verzeichnis

Mitarbeiterbelehrung und Verpflichtung auf den Datenschutz

Jeder Mitarbeiter muß auf den Datenschutz belehrt und verpflichtet werden.

Inhalte: Artikel 5 (Grundsätze), 6 (Rechtmäßigkeit) und 83 (Strafen) Datenschutzverordnung sind Grundwissen

Form: Schriftlich (Dokumentations- und Beweisfunktion)

Hinweis: Sorgen Sie als der Verantwortliche im Unternehmen dafür, dass die Mitarbeiter dies wirklich kennen und beherzigen.

Mitarbeiterbelehrung und Verpflichtung auf den Datenschutz

Verpflichtungserklärung zur Wahrung des Datengeheimnisses (Muster)

Sehr geehrte(r) Frau/Herr

Hiermit verpflichte ich Sie, im Rahmen des Datenschutzes und Ihrer Aufgaben, auf die Wahrung des Datengeheimnisses. Dadurch ist es Ihnen untersagt, im **Rahmen des Arbeitsverhältnisses ohne entsprechende Anweisung personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen.**

Auch über die Dauer Ihrer Tätigkeit hinaus hat diese Verpflichtung Bestand.

Eine Missachtung dieser Vereinbarung kann Sanktionen gemäß der Datenschutz-Grundverordnung (DSGVO) und anderer Gesetze nach sich ziehen. Außerdem kann eine Verletzung dieser Verpflichtung arbeits- oder dienstrechtliche Konsequenzen haben.

.....

.....

Ort, Datum

Unterschrift der verantwortlichen Stelle

Über die notwendigen Pflichten und Verhaltensweisen zum Datenschutz gemäß der DSGVO wurde ich aufgeklärt und habe die entsprechenden Merkblätter erhalten.

.....

.....

Ort, Datum

Unterschrift des Verpflichteten

Informationspflichten

Sehr umfangreiche Informationspflichten

- **Artikel 12 – Information über Rechte der Betroffenen**
- **Artikel 13 - Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person**
- **Artikel 14 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden**

Kunden- oder Betroffenenrechte

- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung und Vergessenwerden
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Recht auf Widerspruch
- Recht darauf, nicht einer Entscheidung auf ausschließlich automatisierter Verarbeitung von Daten unterworfen zu sein (z. Bsp. Scoring!)

Datenschutzbeauftragter

Ein Datenschutzbeauftragter ist zu bestellen

Immer

- wenn Kerntätigkeit bedingt:
- –Regelmäßige und systematische Überwachung der betroffenen Personen
- –Umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten
- –Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten

Kontaktdaten (Adresse, Telefonnummer, E-Mail-Adresse) des Datenschutzbeauftragten sind zu veröffentlichen und der Aufsichtsbehörde mitzuteilen.

Datenschutzbeauftragter

Ein Datenschutzbeauftragter ist auch zu bestellen

- In der Regel sind mindestens 20 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt
- Daten werden verarbeitet, die einer Datenschutzfolgeabschätzung unterliegen, unabhängig von Personenzahl
- Unternehmen verarbeiten Daten zum Zwecke der Markt- und Meinungsforschung, ebenfalls unabhängig von der Personenzahl
- **Kontakt Daten (Adresse, Telefonnummer, E-Mail-Adresse) des Datenschutzbeauftragten sind zu veröffentlichen und der Aufsichtsbehörde mitzuteilen.**

Datenschutzbeauftragter

Ein Datenschutzbeauftragter hat folgende Rechte

- Vorabkontrollen (besonders sensible Datenverarbeitungen)
- Unterrichtung und Beratung des Verantwortlichen für die Datenverarbeitung
- Sensibilisierung und Schulung der Mitarbeiter
- Zusammenarbeit mit der Aufsichtsbehörde
- **Nicht:** Letztverbindliche Entscheidungen

Der Datenschutzbeauftragte ist

- Unabhängig von Weisungen
- Nur mit Zustimmung der Aufsichtsbehörde kündbar (str.)
- **Kontaktdaten (Adresse, Telefonnummer, E-Mail-Adresse) des Datenschutzbeauftragten sind zu veröffentlichen und der Aufsichtsbehörde mitzuteilen.**

Datenschutzpanne/ Datenschutzverletzungen

Wann ist ein Vorfall meldepflichtig?

Die Verordnung verwendet für den umgangssprachlichen Begriff „Datenpanne“ die Bezeichnung **„Schutzverletzung personenbezogener Daten“ (Art. 4 Nr. 12 DSGVO)**. Hiermit ist eine Verletzung der Sicherheit der Datenverarbeitung im weitesten Sinne gemeint.

Vernichtung: alle Formen der Datenlöschung, die Daten unwiederbringlich machen, gleich ob rechtlich unzulässig oder unbeabsichtigt

Verlust: unvorhergesehenes Verlorengelangen von Daten, gleich ob temporär oder dauerhaft

Veränderung: inhaltliches Umgestalten von Daten, Daten erhalten neuen Informationsgehalt

unbefugte Offenlegung / Weitergabe: Dritter erhält Daten, Weitergabe nicht durch Einwilligung oder Rechtsvorschrift gedeckt

unbefugter Zugang: o.; aber auch keine oder fehlerhafte Berechtigungskonzepte können schon dazu führen, da tatsächliche Kenntnisnahme nicht erforderlich ist

Datenschutzpanne/ Datenschutzverletzungen

Wer ist wann über die Datenpanne zu informieren?

Es sind nicht mehr Aufsichtsbehörde und Betroffene gleichermaßen zu benachrichtigen. Die Verordnung enthält anders als § 42a BDSG eine abgestufte Melde- und Benachrichtigungspflicht:

Die Betroffenen müssen – im Gegensatz zur Aufsichtsbehörde – erst dann benachrichtigt werden, wenn durch die Schutzverletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht.

Um die Meldepflicht gegenüber der Aufsichtsbehörde auszulösen, reicht ein „normales“ Risiko, das keiner besonderen Qualifizierung bedarf.

Datenschutzpanne/ Datenschutzverletzungen

Inhalt der Meldung an die Aufsichtsbehörde

- Beschreibung der Art der Verletzung (z.B. Datenverlust)
- Kategorien von Betroffenen (z.B. Mitarbeiter, Kunden)
- (ungefähre) Anzahl der Betroffenen, Kategorien von Datensätzen und ungefähre Anzahl der betroffenen Datensätze (z.B. Datensätze von 351 Kunden und 26 Mitarbeitern betroffen, darunter Anzahl x besonders schützenswerte Daten)
- Name und Kontaktdaten des DSB oder sonstige Anlaufstelle
- Beschreibung der wahrscheinlichen Folgen der Schutzverletzung (z.B. finanzielle Nachteile durch unbefugte Offenlegung von Bank- und Kreditkartendaten)
- Beschreibung ergriffener und vorgeschlagener Maßnahmen, um die Schutzverletzung zu „beheben“ und um mögliche Folgen abzumildern

Datenschutzpanne/ Datenschutzverletzungen

Form der Meldung

Eine besondere Form ist nicht vorgesehen. Gerade in dringenden Fällen bietet sich aber vorab eine telefonische Kontaktaufnahme mit der Aufsichtsbehörde an. Eine ausführliche Meldung, z.B. per Brief oder per Fax, folgt dann dem Gespräch.

Schnelligkeit vor Vollständigkeit

Die (Erst-)Meldung an die Aufsichtsbehörde muss unverzüglich, aber grundsätzlich innerhalb von 72 Stunden erfolgen.

Sonderfall Facebook

- **Die Verantwortlichkeit mit Facebook**
- Unternehmen verwenden für ihre mediale Außendarstellung regelmäßig auch Social-Media-Kanäle. Weit bekannt sind dabei Facebook-Fanpages.
- Unternehmen nutzen Facebook-Fanpages, um ihr Unternehmen Online zu repräsentieren. Über die Fanpage ist es möglich mit den Kunden zu kommunizieren und eine gewisse Beziehung aufzubauen. Facebook stellt interessierten Unternehmen dabei nicht nur seine Plattform zur Verfügung, sondern auch eine Reihe von Auswertungsmöglichkeiten zur Effektivität der Fanpage. Grundlage für die Auswertungen sind zahlreiche Nutzerdaten. In der Vergangenheit wurde die Verantwortlichkeit für die Erhebung und Auswertung von Nutzerdaten eher pauschal bei Facebook gesehen, da letztendlich auch nur Facebook entsprechende Daten erhebt und auswertet.
- Die Frage, wer bei einer Nutzung von Facebook-Fanpages für die Verarbeitung der personenbezogenen Daten der Fanpage-Besucher verantwortlich ist, ist vor kurzem vom [EuGH entschieden](#) worden. Gemäß der Entscheidung des EuGH sind sowohl Facebook als auch das jeweilige Unternehmen oder die jeweilige Einrichtung, die eine Facebook-Fanpage betreiben, gemeinsam für die Verarbeitung der personenbezogenen Daten der Nutzer verantwortlich. Gemäß der Entscheidung des EuGH ist es für eine gemeinsame Verantwortlichkeit nicht relevant, dass jeder Beteiligte in gleichwertiger Art und Weise Einfluss auf die Zwecke und Mittel der Verarbeitung personenbezogener Daten hat. Im Falle von Facebook-Fanpages sei ausreichend, dass der jeweilige Betreiber einer Facebook-Fanpage über bestimmte Einstellungen beeinflussen und entscheiden kann, welche Auswertung erstellt und übermittelt werden.

Sanktionen und Bußgelder

- Art, Schwere und Dauer des Verstoßes sowie Anzahl der Betroffenen maßgeblich
- Verschärfend: Vorsatz und Fahrlässigkeit
- Mildernd: Maßnahmen zur Minderung des Schadens, TOMs
- Höhe richtet sich nach Art des Verstoßes

Abmahnungen

Leichte Fallen!

- Fehlende Datenschutzerklärung auf Homepage
- Veraltete Datenschutzerklärung auf Homepage
- Unvollständige Datenschutzerklärung auf der Homepage (Informationspflicht nach Art. 13 DSGVO zum Zeitpunkt der Datenerhebung beim Betroffenen)
- Fehlende Hinweisschilder auf Videoüberwachung

Hilfsmittel

- Im Web gibt es viele geeignete Vorlagen und Hilfsmittel.
- Empfehlenswert sind die Webseiten der Datenschutzbeauftragten des Bundes und der Länder, die Webseiten der Kammern und Verbände

Inhalt Hinweisschild

Das Schild muss zwingend die folgenden Angaben enthalten:

- **Hinweis auf den Umstand der Beobachtung z.B. durch ein Piktogramm des Kamerasymbols**
- **Angabe der Identität des für die Videoüberwachung Verantwortlichen**
- **Angaben gem. Art. 13 Abs. 1 lit. a, d.h. Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters (dabei genügt die Angabe der Funktion, der Name ist nicht zwingend anzugeben)**
- **Sofern ein betrieblicher Datenschutzbeauftragten bDSB bestellt, sind dessen Kontaktdaten anzugeben, Art. 13 Abs. 1 lit. b**

Hinweisschild

- Das Schild sollte mindestens die Größe DIN A 4 haben

Beispiel für ein vorgelagertes Hinweisschild nach Art. 13 der Datenschutz-Grundverordnung bei Videoüberwachung¹



Weitere Informationen erhalten Sie:

- per Aushang (wo genau?)
- an unserer Kundeninformation / Rezeption / Kasse im Erdgeschoss
- (ggf.) zusätzlich im Internet unter ...

Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters:

Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden):

Zwecke und Rechtsgrundlage der Datenverarbeitung:

berechtigte Interessen, die verfolgt werden:

Speicherdauer oder Kriterien für die Festlegung der Dauer:

¹ Hinweis: Die Informationen sind unentgeltlich in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen. Sie können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden (vgl. Art. 12 DSGVO). Um Lesbarkeit zu erreichen, sollte der Ausdruck mindestens in DIN A4 erfolgen.

Noch Fragen?