



Status des Datenschutzes in der Schweiz

ERFA Kommunikation Efficiency Club vom 30. Juli 2019

Dr. Michael Reinle, LL.M.

Übersicht

- Datenschutzrevision in der Schweiz – wo stehen wir?
- Anwendung der DSGVO auf CH-Unternehmen
- Überblick
- Informationspflichten
- Einwilligung
- Berechtigtes Interesse
- Datenbearbeitungsgrundsätze
- Profiling
- E-Mail Marketing
- Auftragsdatenbearbeitung
- Datenschutz-Folgenabschätzung
- Kompetenzen Datenschutzbehörden



Datenschutzrevision in der Schweiz – wo stehen wir?

Datenschutzrevision in der Schweiz – wo stehen wir?

- **DSG-Revision nicht im luftleeren Raum**
 - Modernisierung der Datenschutzkonvention SEV 108 des Europarates (E-K108)
 - EU-Datenschutzgrundverordnung
- **21. Dezember 2016: Vorentwurf zur Totalrevision des Schweizer Datenschutzgesetzes (DSG) in die Vernehmlassung**
 - Ende Vernehmlassung: 4. April 2017
 - Heftige Kritik am Vorentwurf
- **15. September 2017: Entwurf und Botschaft zur Totalrevision des Schweizer Datenschutzgesetzes**
- **Weiteres Vorgehen**
 - Beratung durch Nationalrat in der Herbstsession 2019 (9.-27. September 2019)

Struktur der Datenschutzrevision

- Beibehaltung der Struktur des Datenschutzgesetzes
- Nur punktuelle Regelung von Big Data (z.B. verstärktes Auskunftsrecht, Data Privacy by Design, Datenschutzfolgenabschätzung, etc.)
- Umstritten, ob Detailregelungen im Gesetz oder durch Selbstregulierung (z.B. Auskunftsrechte und Sorgfaltspflichten) – Verhaltenskodizes durch Berufs- und Wirtschaftsverbände sowie Bundesorgane mit anschl. Stellungnahme durch EDÖB (Art. 10 E-DSG)
- Entscheidend für Umsetzung: Stärkung des EDÖB und Erleichterung des Zugangs zu Gerichten für betroffene Personen (Stärkung der Aufsichtsbehörden in EK-108)
- Umstritten: Sanktionsmechanismus

Anwendung DSGVO auf CH-Unternehmen



Weltweite Anwendung!

- DSGVO gilt weit über Grenzen des Binnenmarkts hinaus: «Extraterritorialität»
- Ort der Datenbearbeitung ist irrelevant
- Keine Niederlassung in EU/EWR erforderlich
- Staatsbürgerschaft der Betroffenen ist nicht entscheidend
- CH wird den Grossteil der Änderungen übernehmen



EU DSGVO ist für Schweizer Unternehmen relevant!

- **Art. 3 DSGVO: Anwendung auch auf Nicht-EU-Unternehmen**
 - Bearbeitung durch Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union, unabhängig davon, ob die Verarbeitung in der Union stattfindet
 - Bearbeitung von Daten betroffener Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht
 - Angebot von Waren und Dienstleistungen an betroffene Personen in der Union
 - Beobachtung des Verhaltens betroffener Personen, soweit ihr Verhalten in der Union erfolgt (Tracking Tools)

Konstellationen

- CH-Unternehmen verfügt über eine **EWR-Niederlassung** und Aktivität der Niederlassung ist untrennbar mit der Aktivität der CH-Haupteinrichtung verbunden
- Verkauf von **Waren oder Dienstleistungen** eines CH-Unternehmens an EU-Kunden oder **Überwachung des Verhaltens von Personen**, sofern sich das Verhalten in der EU abspielt – z.B. **Trackingtools** in Webshop, der auch auf EU-Kunden ausgerichtet ist
- CH-Unternehmen beauftragt EU-Unternehmen zur **Auftragsdatenverarbeitung** (z.B. Cloud-Anbieter) – auch bei Sub-Processing des EU-Verarbeiters an Unternehmen ausserhalb der EU oder Bearbeitung von Personendaten durch CH-Unternehmen **im Auftrag** eines EU-Unternehmens (z.B. einer EU-Niederlassung)



Räumlicher Geltungsbereich – erste Erfahrungen

- Hoher Anteil an E-Commerce-Unternehmen betroffen
- Ausnahme: reiner CH-Onlineshop; **aber Achtung: DSGVO nun auch in Liechtenstein anwendbar**
- Zahlreiche offene Fragen trotz Anwendbarkeit
 - Zwingende Vorgaben für den Sitz des EU-Vertreters?
 - Welche EU-Datenschutzbehörden sind für unterstellte CH-Unternehmen zuständig?



Überblick

Wichtige Themen #1

Räumlicher Anwendungsbereich, Art. 3 EU-DSGVO

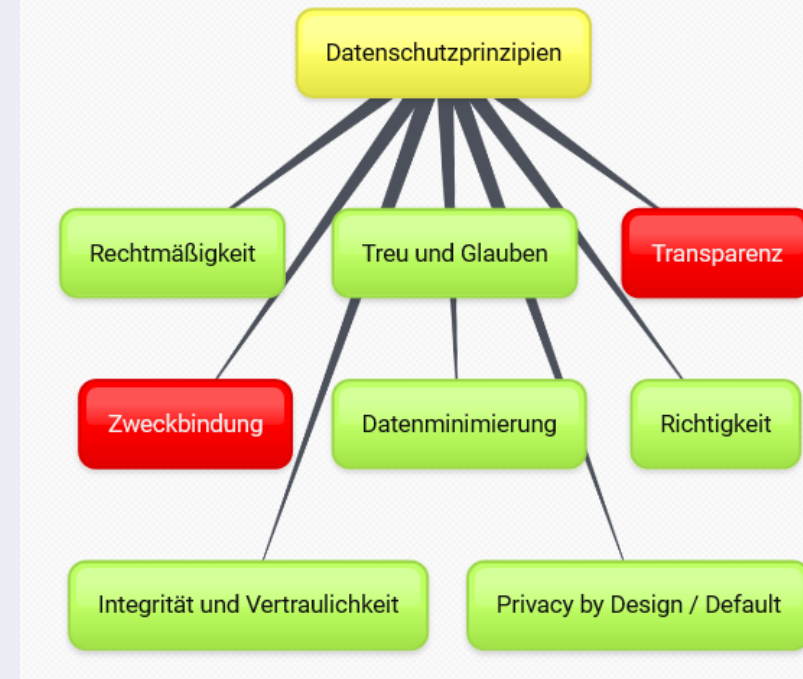
- Datenverarbeitung innerhalb der EU
- Marktortprinzip für Datenverarbeiter mit Sitz in Drittstaaten (z.B. CH)

Grundsatz: Verbot mit Erlaubnisvorbehalt

- Durch die Verordnung selbst
- Durch Einwilligung (hohe Anforderungen an Gültigkeit)
- „überwiegendes Interesse“ (spielt künftig größere Rolle)
- Durch Gesetz

Stärkung der Datenschutzprinzipien, z.B. Transparenz

- Aktive Informationspflicht mit klaren Inhaltvorgaben
- Aktive Informationspflicht auch bei Datenbeschaffung aus Drittquellen
→ Problem bei Datenanreicherung



Wichtige Themen #2

Verschärfte Sorgfaltspflichten

- Datenschutz-Folgenabschätzung („Impact Assessment“),
- Dokumentations- und Nachweispflichten („Accountability“)
- Data Privacy by Design, Data Privacy by Default

Ausbau der Betroffenenrechte

- Auskunftsrecht und Zugriffsrecht
- Recht auf Berichtigung
- Recht auf Löschung einschließlich eines Rechtes auf „Vergessenwerden“
- Recht auf Datenübertragbarkeit (Datenportabilität)
- Widerspruchsrecht und Widerrufsrecht

Deutlich schärfere Sanktionen

- bis zu EUR 20 Mio. oder 4% des weltweiten Jahresumsatzes



Erste Bilanz

Verfahren bei nationalen Datenschutzbehörden

- 206'326 Fälle,
- davon 94'622 durch Beschwerden von betroffenen Personen

Meldungen von Data Breaches

- 64'684

Erste Bussen – Schonfrist vorbei

- EUR 50 Mio. gegen Google durch CNIL (Verletzung Transparenzgebot, ungültige Einwilligung)
- EUR 5'000.00 gegen Kolibri Images durch Datenschutzbehörde Hamburg (fehlender Auftragsverarbeitungsvertrag)
- EUR 2 Mio. gegen Telemarketingunternehmen durch italienische Aufsichtsbehörde
- GBP 99 Mio. gegen Marriott durch britische Aufsichtsbehörde (Data Breach; intention to fine)
- GBP 183 Mio. gegen British Airways durch britische Aufsichtsbehörde (Data Breach; intention to fine)



**Mehr
Bürokratie
wagen!**

Wählt die **PARTEI**. Sie formuliert Formulare.

Die PARTEI

die-partei.net/muenster

Informationspflichten



Direkte Datenbeschaffung

- Informationspflichten, Art. 13 DSGVO bzw. Art. 17 f. E-DSG
 1. **Namen und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters**
 2. Kontaktdaten des Datenschutzbeauftragten
 3. **Zwecke** und Rechtsgrundlage
 4. **Ggf. die berechtigten Interessen an einer Datenverarbeitung**
 5. **Ggf. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten**
 6. Ggf. die Absicht einer Übermittlung in Drittstaaten oder an eine internationale Organisation
 7. **Weitere Informationen, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten**
 8. Dauer der Datenspeicherung bzw. Kriterien für die Festlegung der Dauer
 9. Bestehen von Betroffenenrechten wie Auskunft, Berichtigung, Löschung, Sperrung, Widerspruchsrecht oder Datenübertragbarkeit
 10. Widerrufsrecht bei einwilligungsbasierter Datenverarbeitung
 11. Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
 12. Ggf., ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben ist oder für den Vertragsschluss erforderlich ist
 13. **Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling sowie aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person**

Indirekte Datenbeschaffung

- **Aktive Informationspflicht (Art. 14 DSGVO bzw. Art. 17 Abs. 3 E-DSG)**
 - Informationspflicht gilt auch bei der Beschaffung von Daten aus Drittquellen
 - Information muss spätestens einen Monat nach Datenerhebung aus Drittquelle erfolgen
 - Ausnahme: Information ist unmöglich, unverhältnismässig oder würde den verfolgten Zweck vereiteln

- **Inhalt der Information**
 - a. **den Namen und die Kontaktdaten des Verantwortlichen** sowie gegebenenfalls seines Vertreters;
 - b. zusätzlich die Kontaktdaten des **Datenschutzbeauftragten**;
 - c. **Die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen**, sowie die **Rechtsgrundlage** für die Verarbeitung;
 - d. **die Kategorien personenbezogener Daten**, die verarbeitet werden;
 - e. Gegebenenfalls die **Empfänger** oder **Kategorien von Empfängern der personenbezogenen Daten**;
 - f. gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem **Drittland** oder einer internationalen Organisation zu **übermitteln**,...

Einwilligung



Einwilligung

Definition (Art. 4 Nr. 11 DSGVO):

- freiwillig
- für den bestimmten Fall
- in informierter Weise und
- unmissverständlich abgegebene Willensbekundung
- in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung

Form

- eindeutige bestätigende Handlung
- schriftliche Erklärung, die auch elektronisch erfolgen kann
- „Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen.“ (EG 32) → kein Opt-Out

Alteinwilligungen gelten nur dann, wenn die Anforderungen der DSGVO eingehalten wurden (EG 171)



Einwilligungsgrundsätze

- Art. 7 DSGVO
- Informiertheit (Art. 7 Abs. 2 DSGVO)
 - „Für den konkreten Fall und in Kenntnis der Sachlage“
 - Hervorhebungspflicht bei Verbindung mit anderen Texten (AGB?, DSE?)
 - Klare und einfache Sprache
 - In verständlicher und leicht zugänglicher Form
- Widerruflichkeit (Art. 7 Abs. 3 DSGVO)
 - jederzeit mit Wirkung für die Zukunft widerruflich
 - hierauf ist vor Abgabe hinzuweisen
- Freiwilligkeit (Art. 7 Abs. 4 DSGVO)
 - nicht gegeben bei „klarem Ungleichgewicht“
 - z.B. Zwangssituationen und rechtl. Abhängigkeitsverhältnisse

Einwilligung in Weitergabe von Daten

- OLG Frankfurt vom 28. Juli 2016
 - Einwilligungserklärung in Telefon- und E-Mail-Werbung im Rahmen eines Gewinnspieles unwirksam
 - Grund: Einwilligung für Weitergabe an eine Vielzahl von werbenden Unternehmen zu unbestimmt!
 - Link auf Liste mit 50 werbenden Unternehmen, aber: Geschäftsbereiche der Unternehmen zu wenig spezifisch
- Rechtslage Schweiz
 - Anforderungen an Einwilligung zur Weitergabe von Daten an Dritte liberaler
 - Aber: Nutzer muss eine Vorstellung über den Kreis der Datenempfänger erhalten!
 - Geschäftsbereiche der werbenden Unternehmen auch nach schweizerischem Recht relevant – Kategorisierung genügt!
 - Art. 5 Abs. 6 E-DSG – keine inhaltliche Änderung



Berechtigtes Interesse

Zentraler Erlaubnistatbestand

- **Berechtigtes Interesse als wichtiger Rechtfertigungsgrund für Datenbearbeitungen (Art. 6 Abs. 1 Satz 1 lit. f DSGVO)**
 - Interessenabwägung im Einzelfall: Interesse des Datenbearbeiters gegenüber Persönlichkeitsrechtsinteressen der betroffenen Person
 - Berechtigtes Interesse z.B. bei Bearbeitung von Daten aus Kontaktformularen, um Anfrage zu beantworten
- **Im Zweifel: „Reasonable Expectations“**
 - Mit welchen Datenbearbeitungen musste die betroffene Person im Zeitpunkt der Datenbeschaffung aufgrund der Umstände rechnen!
- **Widerspruchsrecht (Art. 21 DSGVO)**
 - Voraussetzungsloses unentgeltliches Widerspruchsrecht
 - Information der betroffenen Person

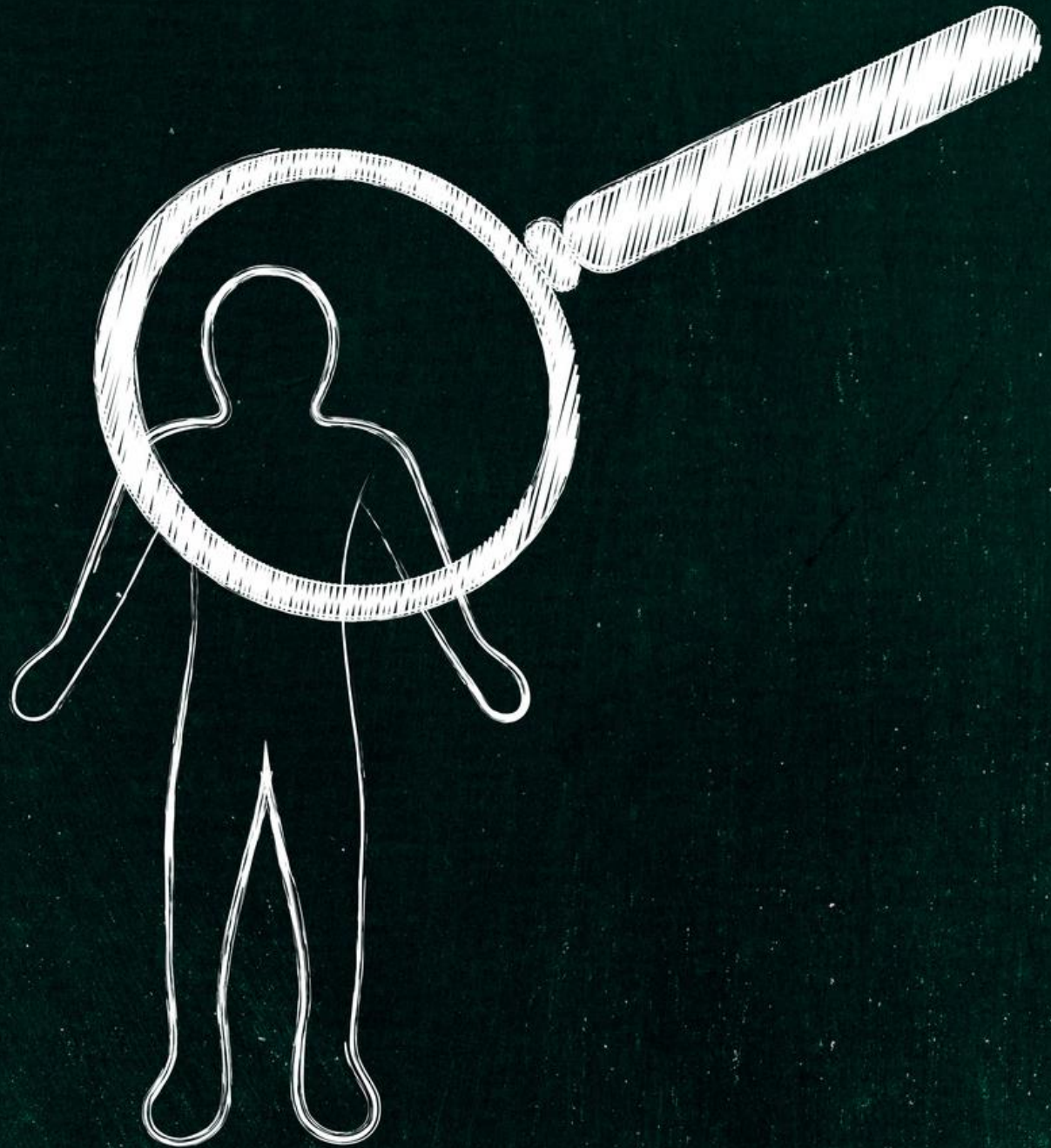
Datenbearbeitungsgrundsätze



Datenbearbeitungsgrundsätze

- **Transparenzgebot (Art. 5 Abs. 3 E-DSG)**
- **Prinzip der Datensparsamkeit (Art 5 Abs. 2 und 4 E-DSG)**
- **Zweckbindungsgebot (Art. 5 Abs. 3 E-DSG)**
- **Richtigkeit der Daten (Art. 5 Abs. 5 E-DSG)**
- **Bearbeitung von veröffentlichten Daten: In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat (Art 26 E-DSG)**

Profiling



Profiling

▪ Art. 4 DSGVO

- **Definition** «Profiling»: jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen
- Keine generelle ausdrückliche Zustimmung für das Profiling; es gilt Art. 6 DSGVO
- Ausdrückliche Zustimmung wird nur in Art. 22 DSGVO im Zusammenhang mit Profiling erwähnt. Dort geht es jedoch um automatisierte Entscheidungen im Einzelfall – inklusive Profiling – mit rechtlicher Wirkung oder erheblicher Beeinträchtigung

Profiling

▪ Art. 4 lit. f E-DSG

- **Definition:** die Bewertung bestimmter Merkmale einer Person auf der Grundlage von automatisiert bearbeiteten Personendaten, insbesondere um die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, das Verhalten, die Vorlieben, den Aufenthaltsort oder die Mobilität zu analysieren oder vorherzusagen
- Geltendes DSG: Persönlichkeitsprofil = eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt
- Unterschied Profiling - Persönlichkeitsprofil
- Praxis des EDÖB betreffend Persönlichkeitsprofile als Interpretationshilfe für Profiling (Quer- vs. Längsprofil)?
- Keine generelle ausdrückliche Zustimmung für das Profiling (eine solche war im VE-DSG noch enthalten)

E-Mail Marketing

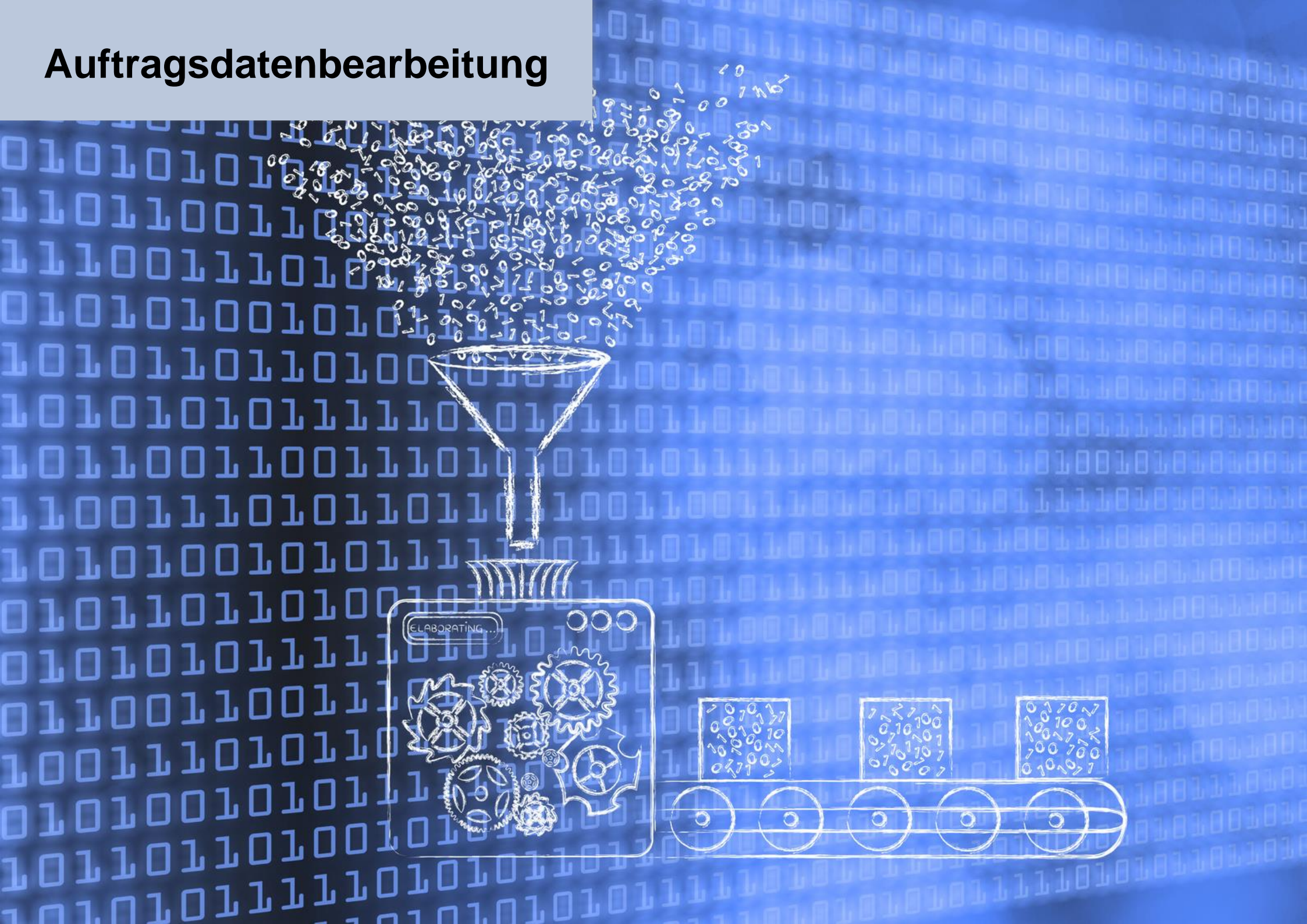
NEWSLETTER



E-Mail Marketing

- **Spamming Verbot (Art. 3 Abs. 1 lit. o UWG)**
 - Keine generelle Erlaubnis zur Zustellung von Newslettern an bestehende Kunden
 - Nicht erlaubt (ohne informierte Einwilligung): Weitergabe für Marketingzwecke an Dritte
 - Im Zweifelsfall: Nur Werbung für eigene Produkte und Dienstleistungen
 - Art. 3 lit. o UWG: Erfasst auch Auftraggeber, nicht nur den Versender
- **Anforderungen an informierte Einwilligung**
 - Tragweite der Einwilligung muss erkennbar sein
 - Betroffene Person muss Vorstellung über den Kreis der Datenempfänger und damit Zusteller von E-Mails haben
 - Einwilligung in AGB zulässig?

Auftragsdatenbearbeitung



Beispiele

- **Google Analytics**
- Cloud-Anbieter für Datenspeicherung
- **Microsoft 365 (Cloud-Lösung)**
- Salesforce / Microsoft Dynamics (CRM-Systeme)
- **Webhoster**

Anforderungen Schweiz (Art. 10a DSG bzw. neu Art. 8 E-DSG)

- Sicherstellung, dass der Auftragsbearbeiter Daten nur so bearbeitet, wie dies die verantwortliche Person auch dürfte
- Instruktions- und Kontrollrechte sowie sorgfältige Auswahl sind besonders wichtig
- Gilt auch bei Auftragsdatenbearbeitungsverhältnissen zwischen inländischen Unternehmen
- E-DSG: Neu Beizug von Subunternehmern nur mit Zustimmung des Verantwortlichen

Anforderungen in der EU (Art. 28 EU-DSGVO)

- Schriftlicher Vertrag
- Genehmigung von Subunternehmern
- Instruktions- und Kontrollrechte des Verantwortlichen
- Unterstützungs- und Kooperationspflichten des Auftragsverarbeiters
- Sorgfältige Auswahl: Zusammenarbeit nur mit Auftragsverarbeitern, die durch die Implementierung von technischen und organisatorischen Massnahmen die Verarbeitung im Einklang mit der EU-DSGVO sicherstellen können
- Sicherstellung der Implementierung von technischen und organisatorischen Massnahmen zur Datensicherheit – **Nachweispflicht des Auftragsverarbeiters**

Beispiel – Inhalt und Zweck eines Datenverarbeitungsvertrag

Inhaltsverzeichnis

Präambel	5
1 Gegenstand	5
2 Einzelheiten des Auftragsinhalts	5
2.1 Art und Zweck der Verarbeitung	5
2.2 Art und Kategorien der Daten	6
2.3 Kategorien betroffener Personen	6
2.4 Ort der Auftragsbringung	6
3 Pflichten des Auftragnehmers	6
3.1 Weisungsgebundenheit	6
3.2 Bestellung eines Datenschutzbeauftragten	7
3.3 Ernennung eines Vertreters mit Sitz in der EU	7
3.4 Aufrechterhaltung der Vertraulichkeit	7
3.5 Unterstützungspflichten	8
3.6 Zusammenarbeit mit der Aufsichtsbehörde	8
3.7 Mitteilung von Verstössen	8
3.8 Meldung von Verletzungen des Schutzes personenbezogener Daten	9
4 Rechte und Pflichten des Auftraggebers	9
5 Technische und organisatorische Massnahmen	10
6 Subunternehmer	11
7 Rechte der betroffenen Personen	12
8 Haftung	13
9 Konventionalstrafe	13
10 Vergütung	14
11 Inkrafttreten und Dauer	14
12 Folgen der Beendigung	14
13 Schlussbestimmungen	14
13.1 Änderungen und Ergänzungen	14
13.2 Integrierende Bestandteile	14
13.3 Gesamte Vereinbarung	15
13.4 Salvatorische Klausel	15
13.5 Anwendbares Recht und Gerichtsstand	15

1. Zweck

Dieser Vertrag wird von und zwischen Muster AG und dem Auftragnehmer abgeschlossen, um einen angemessenen Schutz von Personendaten in Situationen zu gewährleisten, in denen diese Daten von Muster AG an in der Schweiz oder in einem anderen Land niedergelassene Verarbeiter zum Zwecke der Bearbeitung dieser Daten im Namen von Muster AG übermittelt werden.

Ferner unterstützt dieser Vertrag die Parteien bei der Einhaltung der in der Schweiz und der Europäischen Union geltenden Vorschriften über die Bearbeitung von Personendaten, insbesondere der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016, die ab dem 25. Mai 2018 anwendbar ist ("DSGVO").

Die Zwecke, welche mit der Übertragung von Personendaten an den Auftragnehmer und der Verarbeitung durch den Auftragnehmer verfolgt werden, sind in Anlage 1 zu diesem Vertrag beschrieben. Anlage 1 ist integraler Bestandteil dieses Vertrages und kann von Zeit zu Zeit von Muster AG geändert werden.

2. Geltungsbereich

Dieser Vertrag gilt für alle Personendaten, die sich auf Dritte beziehen, und die

- i. von Muster AG an den Auftragnehmer übertragen (miteingeschlossen ist hierbei der Zugriff auf solche Daten) wurden oder
- ii. vom Auftragnehmer im Auftrag von Muster AG bearbeitet werden.

Der Katalog der zu übertragenden und zu bearbeitenden Personendaten ist in Abschnitt 1 von Anlage 1 zu diesem Vertrag enthalten.

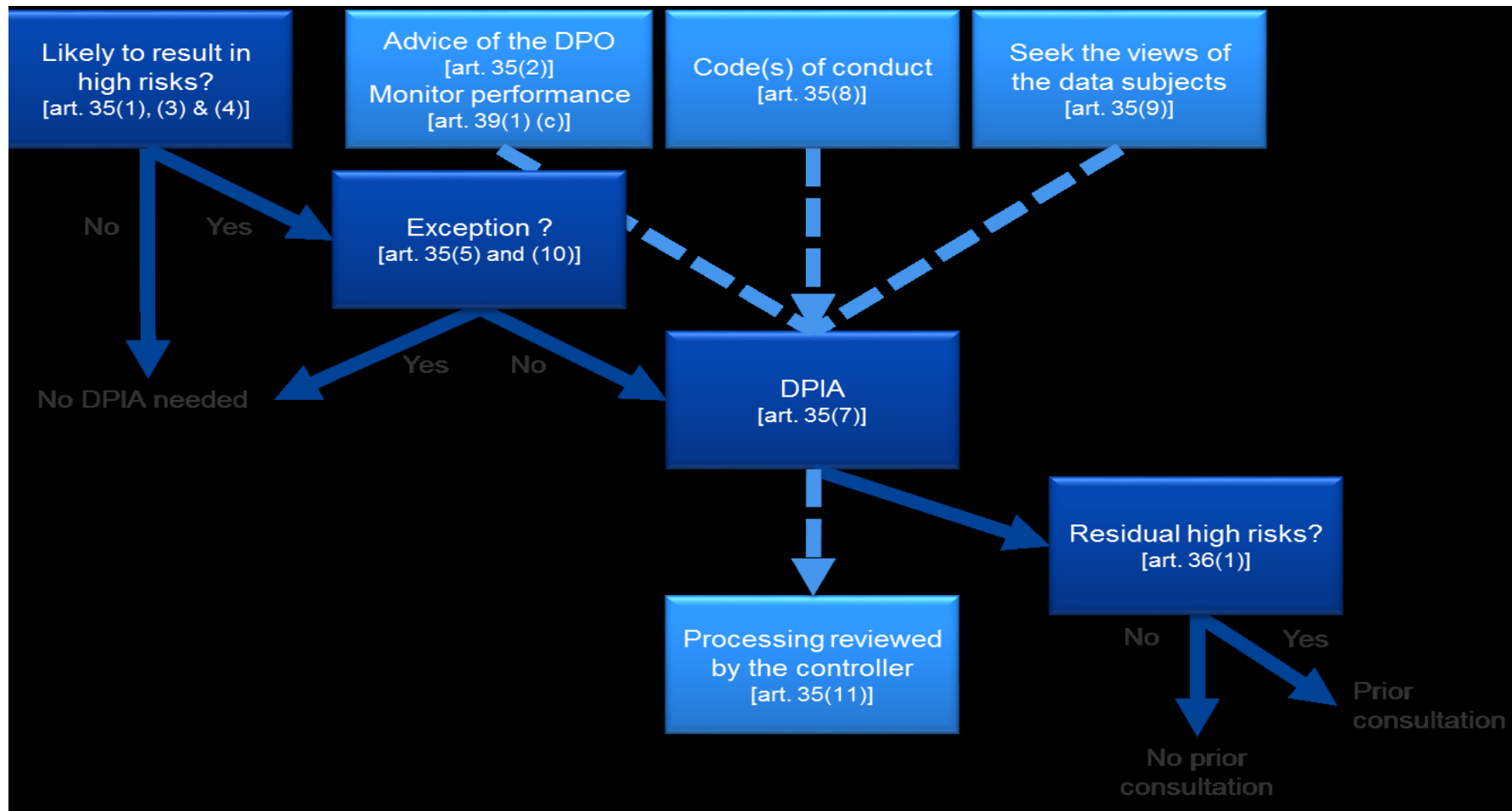


**Datenschutz-Folgen-
abschätzung**

Datenschutz-Folgenabschätzung

- Leitlinien des Europäischen Datenschutzausschusses (EDSA) zur Datenschutz-Folgenabschätzung (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236)
- Aufgreifkriterium: wenn die Verarbeitung „wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt“
- Nationale Datenschutzbehörden: Erarbeitung von „Black Lists“ (https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_de)

Datenschutz-Folgenabschätzung



Quelle: EDSA – Leitlinien zur Datenschutz-Folgenabschätzung

Datenschutz-Folgenabschätzung

Beispiele für Verarbeitungsvorgänge	Ggf. maßgebliche Kriterien	Notwendigkeit einer DSFA wahrscheinlich?
Ein Krankenhaus verarbeitet die genetischen und medizinischen Daten seiner Patienten (Krankenhausinformationssystem).	<ul style="list-style-type: none"> - <u>vertrauliche Daten oder höchst persönliche Daten</u> - Daten zu schutzbedürftigen Betroffenen - Datenverarbeitung in großem Umfang 	Ja
Ein Kamerasystem wird zur Überwachung des Fahrverhaltens auf Schnellstraßen eingesetzt. Zur Identifizierung einzelner Fahrzeuge und automatischen Erkennung von Nummernschildern plant der für die Verarbeitung Verantwortliche den Einsatz eines intelligenten Videoanalyseystems.	<ul style="list-style-type: none"> - systematische Überwachung - innovative Nutzung oder Anwendung technologischer oder organisatorischer Lösungen 	
Ein Unternehmen überwacht systematisch die Tätigkeiten seiner Angestellten, so auch deren Arbeitsplatzrechner, ihre Internetnutzung usw.	<ul style="list-style-type: none"> - systematische Überwachung - Daten zu schutzbedürftigen Betroffenen 	
Aus sozialen Netzwerken werden öffentlich zugängliche Daten erfasst, um daraus Profile zu erstellen.	<ul style="list-style-type: none"> - Bewerten oder Einstufen - Datenverarbeitung in großem Umfang - Abgleichen oder Zusammenführen von Datensätzen - <u>vertrauliche Daten oder höchst persönliche Daten</u> 	
Ein Institut erstellt eine Bonitäts- oder Betrugsdatenbank auf nationaler Ebene.	<ul style="list-style-type: none"> - Bewerten oder Einstufen - automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung - Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert. - <u>vertrauliche Daten oder höchst persönliche Daten</u> 	
Zu Archivierungszwecken werden	<ul style="list-style-type: none"> - vertrauliche Daten 	

Quelle: EDSA Leitlinie zur Datenschutz-Folgenabschätzung

Datenschutz-Folgenabschätzung

Beispiele für Verarbeitungsvorgänge	Ggf. maßgebliche Kriterien	Notwendigkeit einer DSFA wahrscheinlich?
pseudonymisierte personenbezogene vertrauliche Daten zu schutzbedürftigen Betroffenen gespeichert, die an Forschungsprojekten bzw. klinischen Studien teilgenommen haben	<ul style="list-style-type: none"> - Daten zu schutzbedürftigen Betroffenen - Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert. 	
Es werden „personenbezogene Daten von Patienten oder von Mandanten [verarbeitet, wobei die Verarbeitung] durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt“ (Erwägungsgrund 91).	<ul style="list-style-type: none"> - <u>vertrauliche Daten</u> oder <u>höchst persönliche Daten</u> - Daten zu schutzbedürftigen Betroffenen 	Nein
Ein Online-Magazin verwendet eine Verteilerliste, um seinen Abonnenten eine tägliche allgemeine Übersicht zu schicken.	<ul style="list-style-type: none"> - Datenverarbeitung in großem Umfang 	
Ein Online-Händler schaltet auf seiner Website Werbeanzeigen für Oldtimer-Ersatzteile, für die eine Profilerstellung auf der Grundlage von Produkten zum Einsatz kommt, die der Nutzer auf der Website des Online-Händlers angesehen oder gekauft hat.	<ul style="list-style-type: none"> - Bewerten oder Einstufen 	

Datenschutz-Folgenabschätzung

- Wann ist eine Folgenabschätzung durchzuführen: Vor Aufnahme der betreffenden Verarbeitungstätigkeit
- Muss die Folgenabschätzung nur für neue Verarbeitungstätigkeiten durchgeführt werden?
- Vorgehen:
 - Beschreibung des Verarbeitungsvorganges und Verarbeitungszweckes
 - Bewertung der Notwendigkeit und Verhältnismässigkeit der Verarbeitungsvorgänge
 - Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
 - Skizzierung der Massnahmen zur Vermeidung oder Minimierung von Risiken



Kompetenzen Datenschutzbehörden

Kompetenzen gemäss DSGVO

- Art. 58 DSGVO: Umfassende Untersuchungskompetenzen
 - Informationsansprüche gegenüber Verantwortlichen und Auftragsverarbeitern
 - Durchführung von Untersuchungen
 - Überprüfung von Zertifizierungen
 - Hinweise auf Datenschutzverstösse
 - Umfassendes Zugangsrecht zu Daten und Informationen
 - Zugangsrecht zu Räumlichkeiten und Datenverarbeitungsanlagen
- Umfassende Abhilfebefugnisse
 - Verwarnung wegen Datenschutzverstössen
 - Aussprechung von Geldbussen
 - Endgültige oder vorübergehende Beschränkung von Datenverarbeitungen

Kompetenzen gemäss E-DSG

- Umfassende Untersuchungskompetenzen (Art. 43 E-DSG)
 - Durchführung von Untersuchungen
 - Umfassendes Zugangsrecht zu Daten und Informationen
 - Zugangsrecht zu Räumlichkeiten und Datenverarbeitungsanlagen
 - Mitwirkungspflichten des Datenbearbeiters
 - Zeugeneinvernahmen
- Umfassende Abhilfebefugnisse
 - Erlass vorsorglicher Massnahmen, z.B. vorsorglicher Verbote von Datenbearbeitungen (Art. 44 Abs. 2 E-DSG)
 - Verwaltungsmassnahmen, z.B. Anpassung oder Verbot von Datenbearbeitungen, Löschung von Personendaten, Durchführung einer Datenschutz-Folgenabschätzung (Art. 45 E-DSG)

Kompetenzen gemäss E-DSG

- Keine Kompetenz des EDÖB zur Aussprechung von Geldbussen
 - Art. 59 Abs. 2 E-DSG: Kompetenz für Geldbussen bei kantonalen Strafverfolgungsbehörden; EDÖB Recht zur Strafanzeige
- Sanktionierung von Datenschutzverstössen (Art. 54 ff. E-DSG)
 - Normadressaten sind natürliche Personen, gemäss Botschaft die Leitungspersonen
 - Nur bei Vorsatz
 - Maximale Geldstrafe: CHF 250'000.00
 - Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten
 - Verletzung von Sorgfaltspflichten
 - Verletzung der beruflichen Schweigepflicht
 - Missachtung von Verfügungen des EDÖB



Dr. Michael Reinle, LL.M.

Partner, Zürich

michael.reinle@mll-legal.com

www.mll-legal.com | www.mll-news.com

Besten Dank

Wir danken für Ihre Zeit und Ihr Interesse