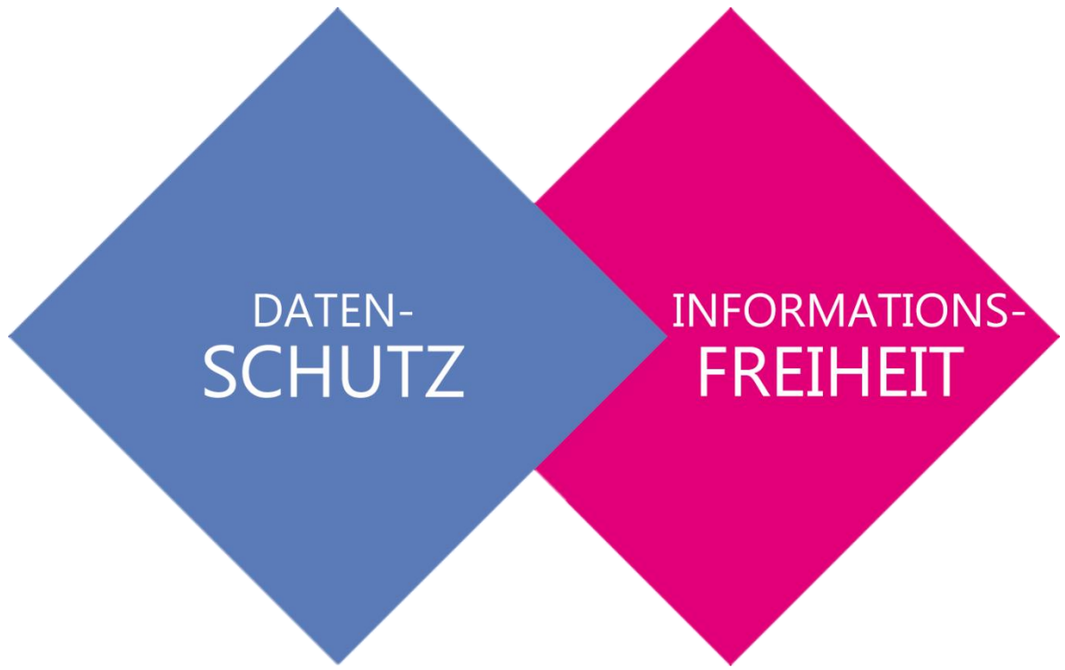

Fragen und Antworten zur EU-Datenschutz-Grundverordnung

Deutsch-Französischer Tag der IT-Sicherheit

14. März 2018

UNABHÄNGIGES DATENSCHUTZ ZENTRUM SAARLAND

Unabhängiges Datenschutzzentrum Saarland

Unabhängiges Datenschutzzentrum

- **Aufsichtsbehörde für die Datenverarbeitung durch nicht-öffentliche und öffentliche Stellen im Saarland**
  - Landesbeauftragte/r für Datenschutz und Informationsfreiheit
  - Wahl durch den Landtag für die Dauer von sechs Jahren
  - bei der Präsidentin/dem Präsidenten des Landtag angegliedert
  - in der Aufgabenausübung völlig unabhängig

(Kern-) Aufgaben des Unabhängigen Datenschutzzentrums

- Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei allen öffentlichen und nicht-öffentlichen Stellen im Saarland
- Verfolgung und Ahndung von Ordnungswidrigkeiten bei Verstößen gegen den Datenschutz
- Unterstützung der Bürger bei der Geltendmachung ihres Anspruchs auf Zugang zu amtlichen Informationen nach dem Saarländischen Informationsfreiheitsgesetz (SIFG)

EU-Datenschutz-Grundverordnung (DS-GVO)

Ziele der DS-GVO

- Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten
- Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten

→ **Europaweit einheitlicher und hoher Datenschutzstandard**

Verordnung (EU) 2016/679 – DS-GVO

- Verordnung gilt verbindlich und unmittelbar in allen Mitgliedstaaten der EU
  - 99 Artikel
  - 173 Erwägungsgründe
- Anwendungsvorrang gegenüber nationalem Recht
- Regelungsbefugnisse der Mitgliedstaaten nur noch in einigen Bereichen:
  - Regelungspflichten
  - Regelungsoptionen

Anpassung im nationalen Recht

- **Neufassung des BDSG** durch das Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU) vom 30.06.2017
  - Inkrafttreten am 25. Mai 2018
  - Maßgebliche Vorschriften für nicht-öffentliche Stellen:
    nur in Teil 1 und Teil 2 (§§ 1 – 44)
    - §§ 1, 2: Anwendungsbereich, Begriffsbestimmungen
    - § 4: Videoüberwachung öffentlich zugänglicher Räume
    - § 26: Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses
    - § 31: Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften
    - § 32 – 37: Rechte der betroffenen Personen
    - § 38 Datenschutzbeauftragte nicht-öffentlicher Stellen

Allgemeine Grundsätze

Anwendbarkeit der DS-GVO

- **Gilt für jede Verarbeitung personenbezogener Daten in der gesamten Europäischen Union**
  - Personenbezogene Daten
    - Informationen, die sich auf identifizierte oder identifizierbare natürliche Person beziehen („betroffene Person“)

      → jede Information, die einer natürlichen Person zugeordnet werden kann
  - Verarbeitung
    - jeder Vorgang, der personenbezogene Daten verwendet
  - Verantwortlicher
    - wer über die Zwecke und Mittel der Verarbeitung entscheidet

Grundsätze für die Datenverarbeitung (Art. 5 Abs. 1 Buchst. a – f)

- **Rechtmäßigkeit der Datenverarbeitung**
  - jede Datenverarbeitung bedarf einer Rechtsgrundlage
    - Einwilligung oder gesetzliche Grundlage (Art. 6 Abs. 1)
- **Transparenz, Treu und Glauben**
  - Gewährleistung einer fairen Verarbeitung
  - Erfordernis der Nachvollziehbarkeit der Verarbeitung der Daten einer betroffenen Person
    - Anforderungen an Art und Weise und Inhalt der Informationen an betroffene Personen (Art. 7 Abs. 2, Art. 12 – 15 und Art. 34)

Grundsätze für die Datenverarbeitung (Art. 5 Abs. 1 Buchst. a – f)

- **Grundsatz der Zweckbindung**
  - Verarbeitung nur für eindeutig festgelegte und dem Betroffenen mitgeteilte Zwecke
  - Kriterien für Zweckänderungen (Art. 6 Abs. 4)
- **Datenminimierung**
  - Verarbeitung auf das notwendige Maß beschränkt
    - Datenschutz durch Technikgestaltung - „Privacy by design“ (Art. 25 Abs. 1)
    - Datenschutz durch datenschutzfreundliche Grundeinstellungen – „Privacy by default“ (Art. 25 Abs. 2)

Grundsätze für die Datenverarbeitung (Art. 5 Abs. 1 Buchst. a – f)

- **Richtigkeit**
  - Sachlich richtig und erforderlichenfalls auf dem neuesten Stand
    - Berichtigungsanspruch (Art. 16)
- **Speicherbegrenzung**
  - Begrenzung der Speicherdauer auf das unbedingt erforderliche Mindestmaß
    - Recht auf Löschung (Art. 17)

Grundsätze für die Datenverarbeitung (Art. 5 Abs. 1 Buchst. a – f)

- **Integrität und Vertraulichkeit**
  - Gewährleistung einer angemessenen Sicherheit der personenbezogenen Daten
    - geeignete technische und organisatorische Maßnahmen zum Schutz vor unbefugter und unrechtmäßiger Verarbeitung und vor unbeabsichtigter Zerstörung (Art. 32)

→ Maßnahmen müssen ein dem Risiko angemessenes Schutzniveau bieten

Rechenschaftspflicht/Accountability

- Der Verantwortliche muss die **Einhaltung der Grundsätze** des Art. 5 Abs. 1 **nachweisen** können (Art. 5 Abs. 2)
- Der Verantwortliche muss sicherstellen und den **Nachweis erbringen** können, dass er **geeignete technische und organisatorische Maßnahmen** umsetzt, damit die Verarbeitung gemäß der Verordnung erfolgt (Art. 24 Abs. 1)

→ Nachweispflicht gegenüber Betroffenen und Aufsichtsbehörden

Rechtmäßigkeit der Datenverarbeitung

Rechtmäßigkeit der Datenverarbeitung (Art. 6)

- **Verarbeitung personenbezogener Daten ist u.a. bei Vorliegen folgender Bedingungen zulässig (Abs. 1):**
  - Einwilligung (Art. 6 Abs. 1 Buchst. a)
  - Erfüllung eines (vor-)vertraglichen Schuldverhältnisses (Art. 6 Abs. 1 Buchst. b)
  - Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen (Art. 6 Abs. 1 Buchst. c)
  - Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten, sofern die Interessen der betroffenen Person nicht überwiegen, insbes. wenn es sich um ein Kind handelt (Art. 6 Abs. 1 Buchst. f)

Einwilligung (Art 4 Nr. 11, 7, 8)

- **Anforderungen an eine Einwilligung**
  - eindeutige bestätigende Handlung, auch elektronisch
  - informiert
  - freiwillig (Koppelungsverbot)
  - verständliche und leicht zugängliche Form in einer klaren und einfachen Sprache
  - Nachweispflicht des Verantwortlichen
- **Einwilligungen Minderjähriger**
- **Fortgeltung von Einwilligungen nach altem Recht**

Informationspflichten

Informationspflichten

- **Rahmenbedingungen (Art. 12)**
  - Form der Unterrichtung
    - leicht zugänglich, auch elektronisch
    - klare und einfache Sprache
  - Frist zur Informationserteilung
    - i.d.R. unverzüglich, in jedem Fall innerhalb eines Monats
- Grundsatz der Unentgeltlichkeit

Informationspflichten

- **Direkterhebung bei der betroffenen Person (Art. 13, § 32 BDSG-neu)**
  - Informationen zum Zeitpunkt der Erhebung
- **Dritterhebung (Art. 14, § 33 BDSG-neu)**
  - Informationen sind innerhalb einer angemessenen Frist nach Erlangung der Daten, spätestens bei der ersten Kontaktaufnahme mit der betroffenen Person zu erteilen

→ **Inhalt**: insbes. Informationen über Art und Umfang der Datenverarbeitung und über Betroffenenrechte

Betroffenenrechte

Rechte der Betroffenen (Art. 12 – 23)

- **Auskunftsrecht (Art. 15, § 34 BDSG-neu)**
  - ob und ggf. welche pb Daten verarbeitet werden
- **Berichtigungsanspruch (Art. 16)**
- **Recht auf Löschung und Recht auf „Vergessenwerden“(Art. 17)**
- **Recht auf Einschränkung der Verarbeitung (Art. 18)**
  - vorübergehender Schutzzustand zur Vermeidung von Nachteilen durch Verarbeitung

Rechte der Betroffenen (Art. 12 – 23)

- **Recht auf Datenübertragbarkeit (Art. 20)**
  - Anspruch auf Mitnahme oder Übermittlung der bei einem Verantwortlichen bereitgestellten personenbezogenen Daten
- **Widerspruchsrecht (Art. 21)**
  - Verarbeitung erweist sich im Nachhinein im Hinblick auf eine Sondersituation als unrechtmäßig und es liegen keine zwingenden schutzwürdigen Gründe für die Verarbeitung vor

    → Korrektur besonderer Einzelfälle (Abs. 1)
  - voraussetzungsloses und uneingeschränktes Widerspruchsrecht bei Datenverarbeitung zum Zweck des Direktmarketings (Abs. 2 und 3)

Pflichten des Verantwortlichen

Pflichten des Verantwortlichen

- **Datensicherheit (Art. 24, 32)**
  - die erforderlichen technischen und organisatorischen Maßnahmen sind an der Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken auszurichten (risikobasierter Ansatz)
  - insbesondere folgende Risiken sind in den Blick zu nehmen:
    - unbeabsichtigte/unrechtmäßige Vernichtung und Veränderung
    - unbeabsichtigter/unrechtmäßiger Verlust
    - unbefugte Offenlegung
    - unbefugter Zugang zu personenbezogenen Daten

Pflichten des Verantwortlichen

- **Datensicherheit (Art. 24, 32)**
  - geeignete Maßnahmen/Ziele u.a.(Art. 32 Abs. 1 Buchst. a bis d):
    - Pseudonymisierung und Verschlüsselung
    - Sicherstellung dauerhafter Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit
    - Wiederherstellung von Verfügbarkeit bei Zwischenfall
    - Verfahren zur regelmäßigen Überprüfung, Bewertung und Wirksamkeit

Pflichten des Verantwortlichen

- **Datenschutzfolgeabschätzung (Art. 35, 36)**
  - sofern eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten des Betroffenen aufweist (risikobasierter Ansatz), insbes. bei:
    - automatisierten Einzelentscheidungen (Scoring)
    - umfangreicher Verarbeitung sensibler Daten
    - Überwachung öffentlich zugänglicher Bereiche
    - umfangreicher Verarbeitung großer Mengen personenbezogener Daten
  - Positiv- und ggf. Negativlisten der Aufsichtsbehörden
  - Gründe für eine Nichtdurchführung sind zu dokumentieren

Pflichten des Verantwortlichen

- **Mindestinhalt der Datenschutzfolgeabschätzung**
  - Beschreibung der geplanten Verarbeitung
  - Bewertung der Notwendigkeit und Verhältnismäßigkeit
    - steht der Eingriff in die Rechte und Freiheiten der Betroffenen im Verhältnis zum Zweck bzw. ist er zum Erreichen des Zwecks erforderlich
  - Risikobewertung
  - Beschreibung der geplanten Abhilfemaßnahmen zum Schutz der personenbezogenen Daten
    - die ermittelten Risiken müssen durch geeignete Maßnahmen eingedämmt werden
- ggf. Beteiligung der Aufsichtsbehörde erforderlich

→ regelmäßige Überprüfung

Pflichten der Verantwortlichen

- **Meldung von Datenschutzverstößen (Art 33, 34)**
  - Meldepflicht binnen 72 Stunden bei der Aufsichtsbehörde, es sei denn voraussichtlich kein Risiko für betroffene Personen

    Mindestinhalt:
    - Beschreibung der Art der Verletzung
    - Name und Kontaktdaten des Datenschutzbeauftragten
    - Beschreibung der wahrscheinlichen Folgen
    - Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen
  - Dokumentationspflicht hinsichtlich aller Verstöße

Pflichten der Verantwortlichen

- **Meldung von Datenschutzverstößen (Art 33, 34)**
  - unverzügliche Benachrichtigung der betroffenen Person, wenn die Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat
  - Ausnahmen von der Benachrichtigungspflicht:
    - Anwendung geeigneter technischer und organisatorischer Vorkehrungen
      (Verschlüsselung)
    - Implementierung von Schutzmaßnahmen
    - unverhältnismäßiger Aufwand: stattdessen öffentliche Bekanntmachung

Pflichten der Verantwortlichen

- **Verzeichnis von Verarbeitungstätigkeiten (Art. 30)**
  - Dokumentation der Verarbeitungsvorgänge
  - Inhalt u.a.
    - Name und Kontaktdaten des Verantwortlichen/Datenschutzbeauftragten
    - Zwecke der Verarbeitung
    - Kategorien von Empfängern
    - Löschfristen
    - Beschreibung der technisch-organisatorischen Maßnahmen
  - auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen
  - Ausnahmen des Art. 30 Abs. 5 liegen selten vor

→ Verzeichnis ist ein wichtiger Baustein der Nachweispflicht

Pflichten der Verantwortlichen

- **Benennung eines Datenschutzbeauftragten (Art. 37)**
  - Kerntätigkeit besteht in der Durchführung von Verarbeitungsvorgängen mit umfangreicher oder systematischer Überwachung von Personen
  - Kerntätigkeit besteht in der umfangreichen Verarbeitung besonders sensibler Daten

→ „Kerntätigkeit" ist die Haupttätigkeit eines Unternehmens, die es untrennbar prägt (ErwGr. 97)

Pflichten der Verantwortlichen

- **Benennung eines Datenschutzbeauftragten (§ 38 BDSG-neu)**
  - es werden i.d.R. mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt
  - es werden Verarbeitungen vorgenommen, die einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO unterliegen
  - es werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet

Pflichten der Verantwortlichen

- **Datenschutzbeauftragter**
  - Berufliche Qualifikation und Fachwissen erforderlich
  - Keine Interessenkollision
  - interne oder externe Bestellung möglich
  - Weisungsfreiheit
  - ordnungsgemäße und frühzeitige Einbindung in alle Datenschutzfragen
  - Veröffentlichung der Kontaktdaten und Mitteilung an die zuständige Aufsichtsbehörde

Auftragsverarbeitung

Auftragsverarbeitung (Art. 28, 29)

- Auftragsverarbeiter muss hinreichende Garantien bieten, dass geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz angewendet werden
- Gesamtverantwortung des Verantwortlichen umfasst auch die Verarbeitung durch den Auftragsverarbeiter
- Haftung auch des Auftragsverarbeiters bei Verstoß gegen Pflichten
- Inhalt des Vertrages (Abs. 3)

Maßnahmenplan

Maßnahmenplan (1/2)

- **Bestandsaufnahme aller Datenverarbeitungen (Ist-Analyse)**
  - Grundlage für Verzeichnis von Verarbeitungstätigkeit
- **Handlungsbedarf ermitteln bzw. Umsetzungsmaßnahmen ergreifen**
  - prüfen, ob und ggf. welche Rechtsgrundlagen für Datenverarbeitungen gegeben sind
    - Überprüfung/Einholung von Einwilligungen
- Implementierung von Maßnahmen zur Gewährleistung von Informationspflichten, Betroffenenrechten und Löschkonzepten
- Implementierung geeigneter Maßnahmen zur Datensicherheit

Maßnahmenplan (2/2)

- Umsetzung der Anforderungen an Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- Überprüfung/Anpassung der Verträge zur Auftragsverarbeitung
- Aufbau einer Dokumentation
- Organisation von Meldepflichten bei Datenpannen
- ggf. Bestellung eines Datenschutzbeauftragten und Meldung an zuständige Aufsichtsbehörde
- Datenschutzfolgeabschätzung durchführen

Haftung und Sanktionen

Haftung und Sanktionen

- **Haftung und Anspruch auf Schadenersatz (Art. 82)**
  - Haftung auch des Auftragsverarbeiters
  - Ersatz des materiellen und des immateriellen Schadens
  - bei Schuldnermehrheit: gesamtschuldnerische Haftung
    → Verantwortlicher muss nachweisen, dass er für den Schaden in keinerlei Weise verantwortlich ist
- **Verbandsklage (Art. 80)**
  - Recht der betroffenen Person, eine Organisation mit der Geltendmachung ihrer Rechte zu beauftragen

Haftung und Sanktionen

- **Verhängung von Geldbußen (Art. 83)**
  - Bußgelder bis zu 4% des weltweiten Jahresumsatzes eines Unternehmens bzw. 20 Mio. Euro
    - Funktionaler Unternehmensbegriff: Mutter- und Tochtergesellschaften werden als wirtschaftliche Einheit betrachtet
  - Zurechnung des Handelns eines Beschäftigten des Unternehmens, nicht wie bisher einer Leitungsperson
  - Bußgelder müssen wirksam, verhältnismäßig und abschreckend sein
    - Art, Schwere und Dauer des Verstoßes
    - Art und Weise des Bekanntwerdens des Verstoßes
    - Zusammenarbeit mit Aufsichtsbehörde

Weiterführende Informationen zur DS-GVO finden Sie unter:

https://datenschutz.saarland.de

Vielen Dank für Ihre Aufmerksamkeit

UNABHÄNGIGES DATENSCHUTZ ZENTRUM SAARLAND

Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Fritz-Dobisch-Straße 12 • 66111 Saarbrücken
Telefon 0681 94781-0
Fax 0681 94781-29
E-Mail:
poststelle@datenschutz.saarland.de
Internet www.datenschutz.saarland.de
www.informationsfreiheit.saarland.de