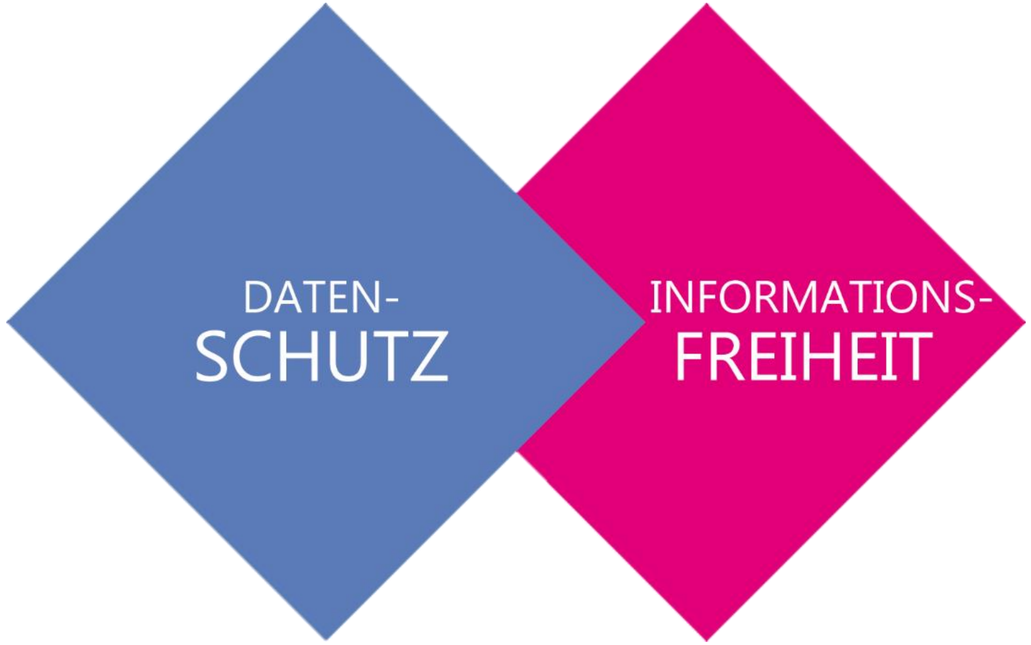

Reform des Datenschutzrechts – das ändert sich ab Mai 2018

Paritätischer Wohlfahrtsverband

10. April 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)

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
    - Art. 88 Datenverarbeitung im Beschäftigungskontext

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**

Anpassung im nationalen Recht

- Änderungen im **Ersten und Zehnten Buch des Sozialgesetzbuches (SGB)** durch Gesetz vom 24.07.2017
  - Redaktionelle Anpassungen an die DS-GVO
    - § 35 SGB I
    - §§ 67 bis 85a SGB X
- Anpassung des **saarländischen Datenschutzgesetzes (SDSG)** Drs. 16/279
  - anwendbar für Datenverarbeitungen durch Behörden und sonstige öffentliche Stellen des Saarlandes
- Anpassung **bereichsspezifischer Vorschriften** in Bund und Ländern

Allgemeine Grundsätze

Begriffsbestimmungen (Art. 4 Nr. 1 – 26)

- **Personenbezogene Daten:** Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person (=betroffene Person) beziehen (ErwGr 26)
- **Verantwortlicher:** Jeder, der allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet
- **Einwilligung:** jede freiwillig, in informierter Weise und unmissverständlich abgegebene Willensbekundung (ErwGr 32)
- **Gesundheitsdaten:** die sich auf die körperliche oder geistige Gesundheit, einschließlich der Erbringung von Gesundheitsdienst-leistungen, beziehen und aus denen Informationen über den Gesundheitszustand hervorgehen (ErwGr 35)

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**
  - 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)
    - Beschränkungen durch nationale Regelungen möglich (Art. 23)
  - Gewährleistung einer fairen Verarbeitung
    - „vernünftige Erwartungen“ der betroffenen Person

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)
    - § 24 BDSG
- **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)
    - ErwGr 43: i.d.R. keine Rgrdl. für Behörden
  - Erfüllung eines (vor-)vertraglichen Schuldverhältnisses (Art. 6 Abs. 1 Buchst. b)
  - 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)
    - gilt nicht für Behörden (Art. 6 Abs. 1 S. 2)

Rechtmäßigkeit der Datenverarbeitung (Art. 6)

- **Präzisierungsmöglichkeiten durch die Mitgliedstaaten (Abs. 2, 3)**
  - Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen (Art. 6 Abs. 1 Buchst. c)
  - Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt (Art. 6 Abs. 1 Buchst. e)
    - § 4 BDSG-neu Videoüberwachung
    - Bereichsspezifische Vorschriften

Besondere Kategorien personenbezogener Daten (Art. 9)

- **Verarbeitung besonderer Kategorien personenbezogener Daten ist grundsätzlich untersagt (Art. 9 Abs. 1)**
  - Datenkategorien
    - rassische und ethnische Herkunft
    - politische Meinungen
    - religiöse und weltanschauliche Überzeugung
    - Gewerkschaftszugehörigkeit
    - genetische Daten
    - biometrische Daten
    - Daten über Gesundheit
    - Daten über Sexualleben und sexuelle Ausrichtung

Besondere Kategorien personenbezogener Daten (Art. 9)

- **Ausnahmen vom Verarbeitungsverbot**
  - unmittelbar nach Artikel 9 Abs. 2, u.a.:
    - Einwilligung (Buchst. a)
    - Tendenzbetriebe (Buchst. d)
    - offensichtlich öffentlich gemachte Daten (Buchst. e)
    - Durchsetzung von Rechtsansprüchen (Buchst. f)
  - aufgrund nationaler Regelungen:
    - Arbeitsrecht (Buchst. b, § 26 Abs. 3 BDSG-neu)
    - Recht der sozialen Sicherheit und des Sozialschutzes (Buchst. b, §§ 22 Abs. 1 Nr. 1 a), 26 Abs. 3 BDSG-neu; SGB)
    - Versorgung im Gesundheitsbereich (Buchst. h, § 22 Abs. 1 Nr. 1 b BDSG)

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

- **Anforderungen an eine Einwilligung (Art. 7)**
  - eindeutige bestätigende Handlung, auch elektronisch
  - informiert
  - freiwillig (Koppelungsverbot)
  - verständliche und leicht zugängliche Form in einer klaren und einfachen Sprache
  - Widerrufbarkeit
  - Nachweispflicht des Verantwortlichen

Informationspflichten und Betroffenenrechte

Rechte der Betroffenen (Art. 12 – 23)

- **Rahmenbedingungen für Betroffenenrechte (Art. 12)**
  - Form der Unterrichtung
    - leicht zugänglich, auch elektronisch
    - klare und einfache Sprache
  - Frist zur Informationserteilung
    - i.d.R. unverzüglich
  - Grundsatz der Unentgeltlichkeit
- **Beschränkung der Betroffenenrechte durch nationale Regelungen möglich (Art. 23)**
  - §§ 29, 32 – 37 BDSG-neu

Informationspflichten des Verantwortlichen

- **Informationspflicht bei Direkterhebung und Dritterhebung (Art. 13, 14, §§ 32, 33 BDSG-neu)**
  - Zeitpunkt der Information
  - Pflichtinformationen: Katalog von Informationen
  - weitergehende Informationen einzelfallbezogen, wenn sie notwendig sind, um eine faire und transparente Datenverarbeitung zu gewährleisten (z.B. Speicherdauer)
  - Mitteilung von Zweckänderungen

→ Dokumentationspflicht

Rechte der Betroffenen (Art. 12 – 23)

- **Auskunftsrecht (Art. 15, § 34 BDSG-neu)**
  - ob und ggf. welche personenbezogenen Daten verarbeitet werden
  - weitergehende Informationen, u.a.
    - Verarbeitungszwecke
    - Empfänger oder Kategorien von Empfängern
    - Dauer der Speicherung
    - Beschwerderecht bei der Aufsichtsbehörde
  - möglichst durch Einrichtung eines Fernzugangs (ErwGr 63)
  - Dokumentation, insbes. bei Auskunftsverweigerung

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

- **Unterrichtung und Verpflichtung von Beschäftigten (Art. 29, 32 Abs. 4)**
  - Verantwortliche und Auftragsverarbeiter müssen sicherstellen, dass ihnen unterstellte Personen personenbezogene Daten ausschließlich auf Weisung verarbeiten
    - Konkrete Verhaltensvorgaben in Form von Betriebs- oder Dienstanweisungen
    - Unterrichtung über datenschutzrechtliche Anforderungen und Verpflichtung zur Wahrung des Datengeheimnisses

Pflichten des Verantwortlichen

- **Verzeichnis von Verarbeitungstätigkeiten (Art. 30)**
  - Dokumentation der Verarbeitungsvorgänge
  - Inhalt (Art. 30 Abs. 1)
    - 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 des 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 des 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 des 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 des 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 des Verantwortlichen

- **Datenschutzbeauftragte**
  - interne oder externe Bestellung möglich
  - berufliche Qualifikation und Fachwissen erforderlich
  - keine Interessenkollision
  - Weisungsfreiheit
  - Verschwiegenheit
  - ordnungsgemäße und frühzeitige Einbindung in alle Datenschutzfragen
  - Veröffentlichung der Kontaktdaten und Mitteilung an die zuständige Aufsichtsbehörde
  - Abberufungs- und Kündigungsschutz

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

Auftragsverarbeitung

Auftragsverarbeitung (Art. 28)

- Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen (Art. 4 Nr. 8 DS-GVO)
  - IT-Dienstleister
  - Speicherung in der Cloud
    - bei Auftragsverarbeitung in Drittstaaten: Art. 44 DS-GVO
  - externe Lohn- und Gehaltsabrechnung
- Auftragsverarbeiter muss hinreichende Garantien bieten, dass geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz angewendet werden
- Inhalte des Vertrags (Art. 28 Abs. 3)

Beschäftigtendatenschutz

Beschäftigtendatenschutz

- **Datenverarbeitung im Beschäftigungskontext (Art. 88)**
  - Abs. 1: Öffnungsklausel für
    - nationale Regelungen
    - Kollektivvereinbarungen: Tarifverträge, Betriebsvereinbarungen
  - Abs. 2: Rahmenbedingungen
  - Allgemeine Datenschutzgrundsätze der DS-GVO gelten
- **Umsetzung in nationalem Recht**
  - § 26 BDSG-neu
  - anwendbar auch auf personenbezogene Daten, die nicht in einem Dateisystem gespeichert sind

Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

- **§ 26 Abs. 1 Satz 1:** Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden
  - soweit dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist
  - oder dies zur Erfüllung der sich aus Gesetz, Tarifvertrag, Betriebs- oder Dienstvereinbarung ergebenden Rechte und Pflichten von Interessenvertretungen erforderlich ist
    - Übermittlung von Daten an Interessenvertretung
    - Verarbeitung von Daten durch Interessenvertretung

Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

- **§ 26 Abs. 1 Satz 2: Datenverarbeitung zur Aufdeckung von Straftaten**
  - zu dokumentierende tatsächliche Anhaltspunkte für den Verdacht einer Straftat
  - Datenverarbeitung erforderlich und keine entgegenstehenden Interessen des Beschäftigten
- **§ 26 Abs. 3 und 4: Verarbeitung besonderer Kategorien personenbezogener Daten**
  - auch auf Grundlage von Kollektivvereinbarungen
  - Verarbeitung muss verhältnismäßig sein und keine überwiegenden entgegenstehenden schutzwürdigen Interessen

Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

- **§ 26 Abs. 2 Einwilligung**
  - Freiwilligkeit:

    Berücksichtigung der im Beschäftigungsverhältnis bestehenden Abhängigkeit sowie der Umstände, unter denen die Einwilligung erteilt wird
    - rechtlicher oder wirtschaftlicher Vorteil für die beschäftigte Person
    - gleichgelagerte Interessen
  - grds. Schriftform erforderlich
  - Aufklärung über Zweck der Datenverarbeitung und Widerspruchsrecht in Schriftform

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
  - Organisation von Meldungen bei Datenpannen

Maßnahmenplan (2/2)

- Implementierung geeigneter Maßnahmen zur Datensicherheit
- Überprüfung/Anpassung der Verträge zur Auftragsverarbeitung
- ggf. Bestellung eines Datenschutzbeauftragten und Meldung an zuständige Aufsichtsbehörde
- Datenschutzfolgeabschätzung durchführen
- Aufbau einer Dokumentation

Haftung und Sanktionen

Haftung und Sanktionen

- **Haftung und Anspruch auf Schadenersatz (Art. 82)**
  - Haftung auch des Auftragsdatenverarbeiters
  - Ersatz des materiellen und des immateriellen Schadens
  - bei Schuldnermehrheit: gesamtschuldnerische Haftung

  →Verantwortlicher muss nachweisen, dass er für den Schaden in keinerlei Weise verantwortlich ist

Haftung und Sanktionen

- **Verhängung von Geldbußen (Art. 83)**
  - Bußgelder bis zu 4% des weltweiten Jahresumsatzes eines Unternehmens bzw. 20 Mio. Euro
  - 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

UNABHÄNGIGES
DATENSCHUTZ
ZENTRUM SAARLAND

Vielen Dank für Ihre Aufmerksamkeit

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