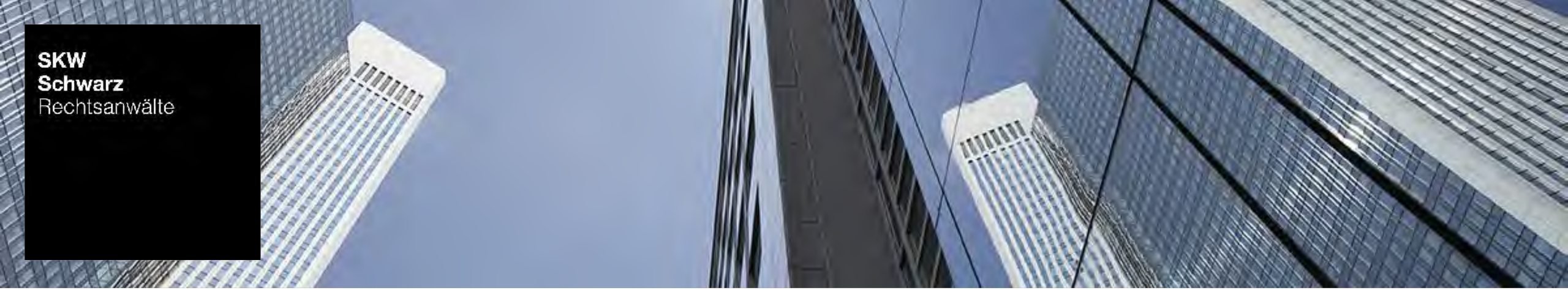


SKW
Schwarz
Rechtsanwälte

Fünf Monate Datenschutz-Grundverordnung – Erste Erfahrungen

Dr. Oliver Hornung

3. IT-Forum Hessenmetall

Kassel, 8. November 2018

SKW Schwarz

SKW Schwarz ist eine unabhängige deutsche Rechtsanwaltskanzlei mit 120 Rechtsanwälten in 5 Büros

120
Rechtsanwälte

16
Beratungsfelder

5
Büros

1
Rechtsanwaltskanzlei

Agenda

01 Einleitung

02 Einführung in die DS-GVO

03 Datenschutz-Grundverordnung – Formelle Pflichten

04 Stellungnahmen der Aufsichtsbehörden zur Umsetzung der DS-GVO

05 Brennpunkte zum aktuellen Datenschutzrecht

01

Einleitung –
Datenschutz-Grundverordnung

Zielsetzung

Erwägungsgrund 11 der Datenschutz-Grundverordnung (DS-GVO)

„Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert eine …

Stärkung und Präzisierung der Rechte der betroffenen Personen

sowie eine

Verschärfung der Auflagen für diejenigen, die personenbezogene Daten verarbeiten und darüber entscheiden,

aber ebenso gleiche Befugnisse der Mitgliedsstaaten bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie gleiche Sanktionen im Falle ihrer Verletzung.“

Einordnung in das Rechtsystem

Vorrang einer EU Verordnung im nationalen Recht

BISHER

- **DATENSCHUTZ-RICHTLINIEN**
- Richtlinie = Umsetzung durch Mitgliedsstaaten mittels nationalem Gesetz
- bspw. RL 95/46 EG
  → Umsetzung im BDSG

NEU

- **VERORDNUNG = UNMITTELBARE GELTUNG IN JEDEM EU-MITGLIEDSSTAAT**
- EU-Verordnung = grds. Anwendungsvorrang vor jedem nationalen Gesetz
  → kein Umsetzungsgesetz im nationalen Recht erforderlich
- Dennoch: Ausgestaltungspflicht durch nationalen Gesetzgeber, sofern durch VO angeordnet

Datenschutz-Grundverordnung

Vorrang einer EU Verordnung im nationalen Recht

Geltung ab dem 25. Mai 2018
Keine Übergangsfrist ab diesem Zeitpunkt

Anpassungsbedarf
→ Interne Dokumentation
→ Neue Begriffe, neue Definitionen, neue Auslegung – selbst bereits im BDSG verwendeter Begriffe

Grundlage: Erwägungsrund (ErwGr.) 171
„innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht“
Einwilligung – Fortgeltung, sofern entsprechend der DS-GVO erteilt
Sonderregelung für Entscheidungen/Beschlüsse der EU-Kommission

02

Einführung in die DS-GVO

Personenbezogene Daten

Zu unterscheiden ist grundsätzlich zwischen:

Personenbezogenen Daten

– „personenbezogene Daten“ sind alle Informationen, die sich auf eine **identifizierte** oder **identifizierbare** natürliche Person beziehen“, Art. 4 Nr. 7 DS-GVO

– Erfasst ist nicht nur der Klarname, sondern auch solche Informationen, die mit Hilfe von **Zusatzwissen** Rückschlüsse die Identität erlauben

– Beispiele personenbezogener Daten sind **Personalien** (Name, Adresse und andere Kontaktdaten, Geburtstag und -ort sowie Staatsangehörigkeit), (Ausweise und amtliche Dokumente) und **Legitimations-Authentifikationsdaten** (Unterschriftprobe), **Werbe- und Vertriebsdaten** (inkl. Werbescores) sowie **Dokumentationen** (etwa Protokolle aus Besprechungen)

Besondere Kategorien personenbezogenen Daten

– Besondere Kategorien personenbezogener Daten sind abschließend im Gesetz definiert

– Erfasst sind Informationen über die **rassische** und **ethnische** Herkunft, **politische** Meinungen, **religiöse** oder **weltanschauliche** Überzeugungen oder die **Gewerkschaftszugehörigkeit**, **genetischen** und **biometrischen** Daten, **Gesundheitsdaten** und Informationen über die **sexuelle** Orientierung

– Verarbeitung ist nur nach den (strengen) Vorgaben des Art. 9 DS-GVO erlaubt

Grundprinzipien der DS-GVO

Im weiteren Sinne Prinzipien des Art. 5 DS-GVO

- **Rechtsmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**
  - Erfüllung der Informationspflichten
  - Schaffung vernünftiger Erwartungen gemäß EG 47
- **Zweckbindung**
  - Sicherstellung durch Informationspflichten
- **Datenminimierung**
  - Sicherstellung durch Verfahrensdokumentationen /-verzeichnisse
  - Löschroutinen

Grundprinzipien der DS-GVO

Im weiteren Sinne Prinzipien des Art. 5 DS-GVO

- **Richtigkeit**
  - Sicherstellung durch (automatisierte) Aktualisierungsmechanismen
- **Speicherbegrenzung**
  - Umsetzung durch technische Löschfristen
  - Unbestimmter Rechtsbegriff der Erforderlichkeit
  - Vgl. Code of Conduct der Wirtschaftsauskunfteien
- **Neu:** Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO
  - Führt zur Beweislastumkehr
  - Aufsichtsbehördliches Vorgehen: „Zeigt mal“

Sanktionsrahmen

Massive Verschärfung gegenüber altem Bundesdatenschutzgesetz

Art. 83 Abs. 4	**Art. 83 Abs. 5**	**Art. 83 Abs. 6**	**Art. 82 Abs. 1**
bis 10 Mio. € oder bis 2% des weltweiten Vorjahresumsatzes	bis 20 Mio. € oder bis 4% des weltweiten Vorjahresumsatzes	bis 20 Mio. € oder bis 4 % des weltweiten Vorjahresumsatzes	Haftung und Recht auf Schadensersatz
je nachdem, was höher ist (!)			Noch nicht absehbar
Verstöße gegen Regelungen zu z. B. • Schutzmaßnahmen (technisch-organisatorische Maßnahmen) • Auftragsverarbeitung (NEU: auch gegen Auftragsverarbeiter)	Verstöße gegen Regelungen zu z. B. • Grundsätze (Art. 5) • Rechtmäßigkeit	Verstöße gegen Anordnungen der Aufsichtsbehörde	Grundsätzlich jegliche Verstöße gegen die Verordnung Kompensation jeglichen materiellen und immateriellen Schadens
Nach Erwägungsgrund 148 der Datenschutz-Grundverordnung sollen Verstöße grundsätzlich auch mit Bußgeldern geahndet werden, außer es würde eine **besondere Härte** für die verantwortliche Stelle darstellen. Höhe des Bußgelder ist **einzelfallabhängig** und zieht eine **Vielzahl von Indikatoren** mit ein wie Grad des Verschuldens, Mithilfe bei der Sachverhaltsaufklärung oder wirtschaftliche Leistungsfähigkeit. Alternativ kommen auch **andere Maßnahmen** nach Art. 58 DS-GVO in Betracht wie **Ordnungsverfügungen**.			

Verbot mit Erlaubnisvorbehalt

Überblick: Rechtsgrundlagen der Datenverarbeitung

Jede Datenverarbeitung ist verboten, es sei denn, das Gesetz erlaubt diese

Rechtsgrundlagen der Datenverarbeitung insbesondere in Art. 6 DS-GVO enthalten

- Datenverarbeitung zur **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, Art. 6 Abs. 1 lit. b DS-GVO
  Beispiel: Jegliche Informationen für die Abrechnung wie Speisen und Getränke oder Sonderleistungen wie Spa

- Datenverarbeitung ist erforderlich für die **Erfüllung einer rechtlichen Verpflichtung**, der der Verantwortliche unterliegt, Art. 6 Abs. 1 lit. c DS-GVO
  Beispiel: Speicherung von Daten zur Erfüllung steuerrechtlicher Pflichten

- Datenverarbeitung ist für die **Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten** erforderlich, Art. 6 Abs. 1 lit. f DS-GVO
  Wichtiger Hinweis: Interessensabwägung ist zu **dokumentieren**

- Datenverarbeitung aufgrund einer **Einwilligung** der betroffenen Person, Art. 6 Abs. 1 lit. a DS-GVO
  Wichtiger Hinweis: **Alt-Einwilligungen** nach dem BDSG gelten weiter, soweit sie rechtmäßig eingeholt worden sind

Typische Verarbeitungsvorgänge beim Betrieb eines Unternehmens

Kundenbezogene Datenverarbeitung am Beispiel CRM-System

Pflege des CRM-System

- **Verarbeitung personenbezogenen Daten im CRM-System**
  - Keine expliziten Regeln für CRM-Systeme im Gesetz enthalten
  - Maßstab ist Art. 17 Abs. 1 lit. a DS-GVO sowie Art. 5 Abs. 1 lit. c DS-GVO
  - Hiernach gelten die Prinzipien der **Erforderlichkeit** sowie **Datenminimierung**

- **Speicherung** personenbezogener Daten nur, soweit dies zur **Durchführung des Vertragsverhältnisses** erforderlich oder durch **Gesetz** gefordert ist; hierzu gehören insbesondere
  - Name, Kontaktdaten (postalische Adresse, E-Mail und ggf. Telefon),
  - Zahlungsinformationen sowie
  - sonstige Informationen (**aber**: Grundsatz Datenminimierung beachten)

- **Darüber hinausgehende** Speicherung personenbezogener Daten nur aufgrund expliziter **Einwilligung** zulässig; hierzu gehören insbesondere
  - KfZ-Kennzeichen
  - Sonderwünsche und Vorlieben
  - Angaben zur Gesundheit
  - Angaben zu minderjährigen Begleitpersonen (unter 18 Jahren)

Handlungsempfehlung: CRM-System sollte zwischen Daten zur Durchführung des Vertrages oder aufgrund Gesetz einerseits sowie solchen Daten unterscheiden, die aufgrund einer Einwilligung gespeichert werden.

Typische Verarbeitungsvorgänge beim Betrieb eines Unternehmens

Kundenbezogene Datenverarbeitung am Beispiel eines Newsletters

Werbemaßnahmen (Newsletter)

- Verarbeitung personenbezogenen Daten wie E-Mail-Adressen für **Werbezwecke**
  - Keine expliziten Regeln für Werbemaßnahmen in der DS-GVO enthalten
  - Rechtsgrundlage ist wiederum Art. 6 Abs. 1 lit. f DS-GVO
  - Ausgangspunkt der Interessensabwägung ist Erwägungsgrund 47:

    „*Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.“*

- **Werbemaßnahmen** sind hiernach für **Bestandskunden erlaubt**, wenn **kein umfangreiches Interessensprofil** erstellt wurde und die betroffene Person hinreichend informiert wurde

- Trotz (gesetzlicher) Erlaubnis hat betroffene Person ein **jederzeitiges** und **nicht zu begründendes Widerspruchsrecht** nach Art. 21 DS-GVO, auf das durch den Verantwortlichen explizit **hinzuweisen** ist; Folge des Widerspruchs ist das Verbot der Verarbeitung der Daten für Werbezwecke

- **Ergänzend** gelten die Regeln des **Gesetzes gegen den unlauteren Wettbewerb** (UWG)
  - Erfasst jegliche „*Werbung unter Verwendung elektronischer Post*“
  - Werbemaßnahmen insbesondere nur zulässig für **Kunden** sowie bei **Hinweis auf jederzeitiges Widerspruchsrecht** der Verwendung der Kontaktinformationen für Werbezwecke

Typische Verarbeitungsvorgänge beim Betrieb eines Unternehmens

Kundenbezogene Datenverarbeitung mit Einwilligung

Beispiel für datenschutzrechtliche Einwilligung für Werbemaßnahmen

- Maßgebliche Regelung ist Art. 7 DS-GVO
- **Mindestanforderungen** sind
  - Hinweis auf **Widerrufsrecht** nach Art. 21 DS-GVO
  - Verständliche und leicht zugängliche Form, aber: **Keine gesetzlichen Formerfordernisse**: Schriftform (Unterschrift) genauso zulässig wie Textform (E-Mail); Aufsichtsbehörden fordern jedoch **kein Medienbruch**
  - Klare und einfache Sprache: Übersetzung in die **jeweilige Landessprache**
  - Transparenz- und Hervorhebungsgebot: Nicht mit anderen Erklärungen und Texten verbinden: **Optische Hervorhebung** und **separate Abfrage**
  - **Zeitpunkt** der Einwilligungserklärung: Vor der (ersten) Erhebung personenbezogener Daten (keine nachträgliche Legitimierung)
- **Rechenschaftspflicht** für das Bestehen einer Einwilligung nach Art. 5 Abs. 2 DS-GVO: Dokumentation jeder Einwilligung

Anmeldung für den [Hotel]-Newsletter

Ja, ich möchte den Newsletter des [Hotel] mit auf mich zugeschnittenen Informationen über Produkte [ggf. spezifizieren] und Aktionen des [Hotel] und [Hotel]-Partnerunternehmen abonnieren:

Geben Sie hier Ihre E-Mail-Adresse ein

ZUM NEWSLETTER ANMELDEN

Diese Einwilligung können Sie jederzeit, z.B. hier [Mit Link zur Newsletter-Abmeldung versehen] oder am Ende jedes Newsletters widerrufen, was zu

einer Löschung der erhobenen Nutzerdaten führt.

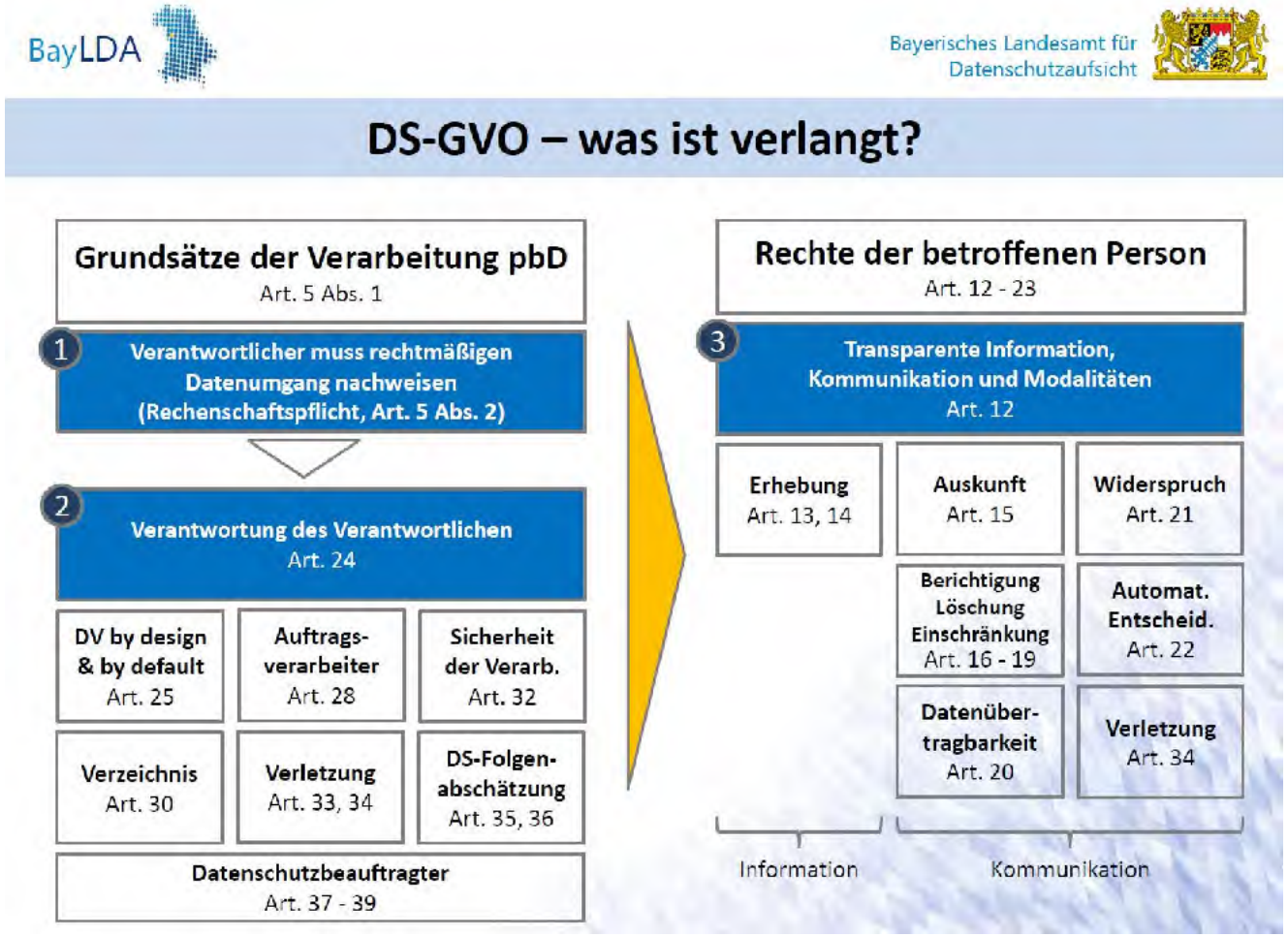
Weitere Informationen finden Sie in unseren Datenschutzbestimmungen [Mit Link zu den Datenschutzbestimmungen versehen].

03

Datenschutz-Grundverordnung –
Formelle Pflichten

DS-GVO – Was wird verlangt?

Am Beispiel des Bayerischen Landesamtes für Datenschutzaufsicht



Quelle: Bayrisches Landesamt für Datenschutzaufsicht

BDSG-alt – Bisherige Prüfpraxis

Am Beispiel des Bayerischen Landesamtes für Datenschutzaufsicht

BayLDA Statistik	2013	2014	2015	2016	2017	2018 (01.01-17.09)	2018	2018	Trend
						Summe	davon bis 25.Mai	davon seit 25.Mai	
Beratungen Vereine, Unternehmen	1733	1821	1850	2003	2974	6629	3834	2795	↑↑
Beratungen Privatpersonen	799	991	977	1065	1104	772	399	373	→
Beschwerden	925	953	1103	1424	1707	2229	731	1498	↑
Bußgeldverfahren	53	64	94	79	78	82	49	33	→
„Datenpannen“	32	21	28	85	150	1231	92	1139	↑↑↑

Quelle: Bayrisches Landesamt für Datenschutzaufsicht

DS-GVO – Neue Prüfpraxis

Am Beispiel des Bayerischen Landesamtes für Datenschutzaufsicht

- Unser Plan für Prüfungen ist konkret:
  - 09.2018: Prüfung **Rechenschaftspflicht** von (erstmal drei) Großunternehmen
  - 09.2019: **Cybersicherheit**: Verschlüsselungstrojaner bei Arztpraxen (erstmal 8 Praxen)
  - 10.2018: Erfüllung der Informationspflichten in **Bewerbungsverfahren** (bei erstmal 25 Unternehmen)
  - 10.2018: **Cybersicherheit**: Patch-Management bei (erstmal 15) Online-Diensten
  - 11.2018: **Cybersicherheit**: Erkennung von Datenschutzverletzungen bei internationalen Sub-Dienstleistern (erstmal 5 Großunternehmen)
  - 12.2018: …

DS-GVO – Neue Prüfpraxis

Am Beispiel der Niedersächsischen Landesdatenschutzsicht

Presse

Die Landesbeauftragte für den Datenschutz Niedersachsen

29.06.2018

Fragen zur DS-GVO an 50 Unternehmen

Landesbeauftragte prüft, wie gut Niedersachsens Wirtschaft die neuen Datenschutzregeln umsetzt

Informationspflichten

Übersicht

UNTERSCHEIDUNG DER UNTERRICHTUNG

Art. 13: Informationspflichten **zum Zeitpunkt der Erhebung** (Geltung auch für Einwilligung)

Art. 14: Wenn die Daten **nicht bei der betroffenen Person erhoben** werden

ERWEITERUNG DES INHALTS

insbesondere:
NEU: Name des Verantwortlichen
NEU: Kontaktdaten des/der Datenschutzbeauftragten
NEU: Zweck der Verarbeitung sowie Rechtsgrundlage
NEU: das berechtigte Interesse (Art. 6 Abs. 1 lit. f), sofern darauf beruhend
NEU: Hinweis auf Widerspruchsrecht (auch bei Einwilligung)
NEU: Absicht der Drittlandübermittlung und einen Hinweis auf die Grundlage der Zulässigkeit der Drittlandübermittlung

KONSEQUENZ UND HERAUSFORDERUNG

Erhebliche Umgestaltung der Informationen

Informationspflichten

Müssen auch Bestandskunden informiert werden?

- Nach Ansicht der Bayerischen Landesdatenschutzaufsicht grundsätzlich nicht
- Aber: Dieses setzt ordnungsgemäße (und nachweisbare) Mitteilung der Pflichtinformationen an die Bestandskunden vor dem 25. Mai 2018 voraus

FAQ zur DS-GVO

Bayerisches Landesamt für Datenschutzaufsicht

Frage	Muss ein Verein seine „Bestandsmitglieder" über die Datenschutz-Grundverordnung informieren? Wenn ja, wie und wann?
Stichworte	Informationspflicht bei Vereinen
Norm	Art. 12, 13 DS-GVO
Antwort	Die in den Artikeln 12 - 14 DS-GVO geregelte Pflicht des Verantwortlichen zur Information der betroffenen Personen über die Verarbeitung ihrer Daten muss nach dem Gesetzeswortlaut zum Zeitpunkt der Datenerhebung erfüllt werden. Gegenüber Mitgliedern, deren Daten der Verein bereits vor dem 25.05.2018 (d.h. vor dem Geltungsbeginn der DS-GVO) erhoben hat („Bestands-mitglieder"), müssen die o.g. Informationen somit grundsätzlich nicht erteilt werden. Hingegen müssen (Neu-)Mitglieder, die ab dem 25.05.2018 in den Verein eintreten, entspre-chend informiert werden, beispielsweise durch Mitteilung der Informationen im Aufnahmeantrag oder in einem Beiblatt. Vorstellbar ist auch, auf einem elektronischen Antragsformular zumindest

Quelle: Bayrisches Landesamt für Datenschutzaufsicht

Informationspflichten

Muster zur Erfüllung der Informationspflichten, hier: Videoüberwachung

Datenschutzhinweise zur Videoüberwachung

ACHTUNG
VIDEOÜBERWACHUNG

Diese Informationen finden Sie zusätzlich auf unserer Internetseite:
[…]

Spaltenumbruch

Name und Kontaktdaten des Verantwortlichen:

[…]

Kontaktdaten des Datenschutzbeauftragten:

[…]

Zwecke und Rechtsgrundlage der Datenverarbeitung:

Schutz der Rechte des Verantwortlichen sowie von Kunden, Besuchern und anderen Personen (Art. 6 Abs. 1 lit. f DSGVO)

Berechtigte Interessen, die wir verfolgen:

Wir führen die Videoüberwachung zur Wahrnehmung des Hausrechts, zum Schutz vor Einbrüchen, Diebstählen oder Vandalismus, zu Gewährleistung der Compliance mit gesetzlichen Vorgaben (z.B. zollrechtlichen Vorschriften) und zur Sammlung von Beweismitteln bei Straftaten.

Weitergabe von Aufzeichnungen:

Personenbezogene Daten werden an andere Verantwortliche nur dann übermittelt, soweit wir aufgrund gesetzlicher Bestimmungen oder durch vollstreckbare behördliche bzw. gerichtliche Anordnung hierzu verpflichtet sein sollten.

Abschnittswechsel (Fortlaufend)

Speicherdauer oder Kriterien für die Festlegung der Dauer:

Die Speicherdauer orientiert sich an den oben genannten berechtigten Interessen und beläuft sich grundsätzlich auf höchstens 72 Stunden.

Informationspflichten

Was müssen Unternehmen jetzt tun?

Informationspflichten jetzt prüfen und umsetzen!

Informationspflichten insbesondere relevant für 3 **Bereiche**
- **Kunden, Interessenten** und **Lieferanten**,
- **Bewerber** und **Beschäftigte** sowie
- **Online-Bereic**h im Rahmen der Webseite.

Grundsätzlich **keine Formvorgaben**, das heißt Erfüllung durch
- **Aushang** im Unternehmen (z. B. im Eingangsbereich),
- **Anlage** zum Vertrag,
- **Auslage** auf dem Empfangstresen zum Mitnehmen oder
- als **Dokument** auf der **Webseite.**

Erfüllung der Informationspflichten muss **nachgewiesen** werden können, Art. 5 DS-GVO
- **Empfehlung:** Hinweis/Link auf Datenschutzerklärung der Website im Rahmen der E-Mail-Signatur von Mitarbeitern!

Bei internationaler Tätigkeit
- **Übersetzung** in die jeweilige Landesprache

Betroffenenrechte

Unter „Rechten der betroffenen Person“ versteht das Datenschutzrecht die Rechte jedes Einzelnen gegenüber für die Verarbeitung Verantwortlichen.

- Auskunft Art. 15 DS-GVO (sehr umfassende Auskunftspflicht, Recht auf Erhalt einer Kopie der Daten)
- Berichtigung Art. 16 DS-GVO
- Löschung Art. 17 DS-GVO („Recht auf Vergessenwerden“)
- Einschränkung der Verarbeitung Art. 18 DS-GVO
- Recht auf Datenübertragbarkeit Art. 20 DS-GVO
- Widerspruchsrecht Art. 21 DS-GVO
- Recht, nicht einer ausschließlich automatisierter Verarbeitung, einschließlich Profiling zu unterliegen, Art. 22 DS-GVO

- **Tipps für Vorgehensweise:**
  - Entwicklung eines Prozesses zum Beschwerdemanagement
  - Erstellung von Muster-Schreiben an die betroffenen Personen zur Erfüllung einzelner Ansprüche

Verarbeitungsverzeichnisse

Übersicht – Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO

– Grundsätzlich besteht Pflicht für Verantwortlichen nach Abs. 1 als auch für Auftragsverarbeiter nach Abs. 2

Ausnahmen für Unternehmen bis 250 Mitarbeitern, sofern
- die Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, nur gelegentlich erfolgt oder nicht besondere Datenkategorien einschließt.
- Achtung: Regelmäßige Verarbeitung von Gesundheitsdaten und somit besondere Datenkategorien durch Personalabteilung

Folge: Regelmäßig keine Befreiung von dieser Pflicht!

– **Keine Herausgabepflicht** an Jedermann (sogenanntes „*Jedermannsverzeichnis*“)

– **Unterschiedliche Inhalte** für Verantwortlichen und Auftragsverarbeiter

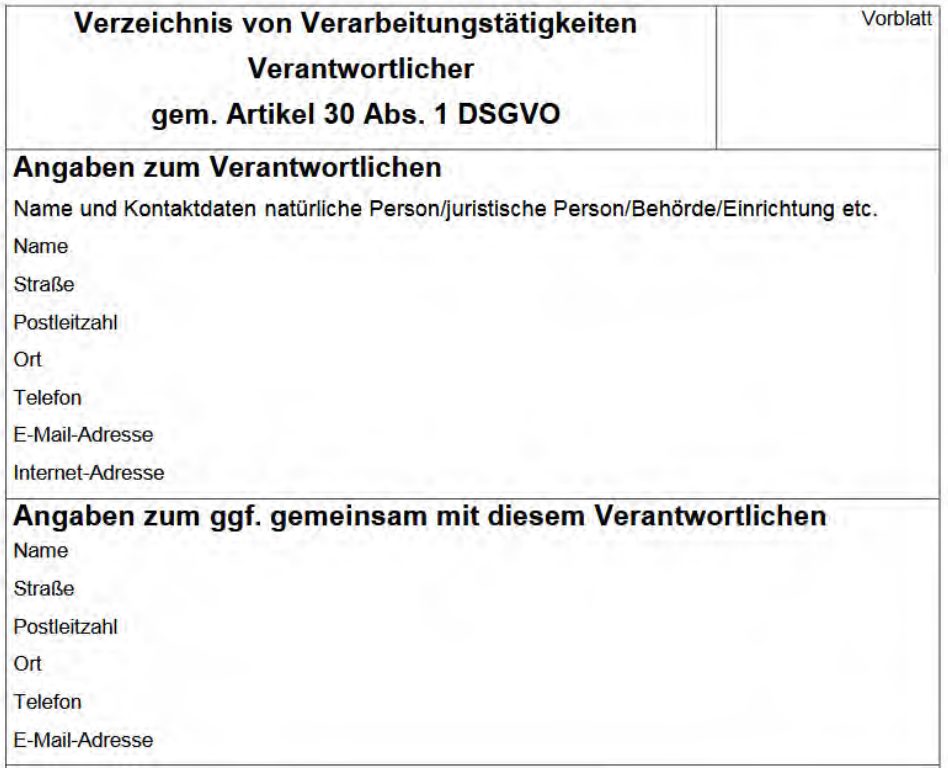
– Gegenüber Aufsichtsbehörde auf **Anforderung** zur Verfügung stellen

– Aufzeichnungen sind schriftlich zu führen, **elektronisches Format** genügt

Verarbeitungsverzeichnisse

Übersicht – Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO

Muster für Verzeichnisse auf den Webseiten der Landesaufsichtsbehörden in Bayern und Hessen:



Verzeichnis von Verarbeitungstätigkeiten
Verantwortlicher
gem. Artikel 30 Abs. 1 DSGVO

Vorblatt

Angaben zum Verantwortlichen

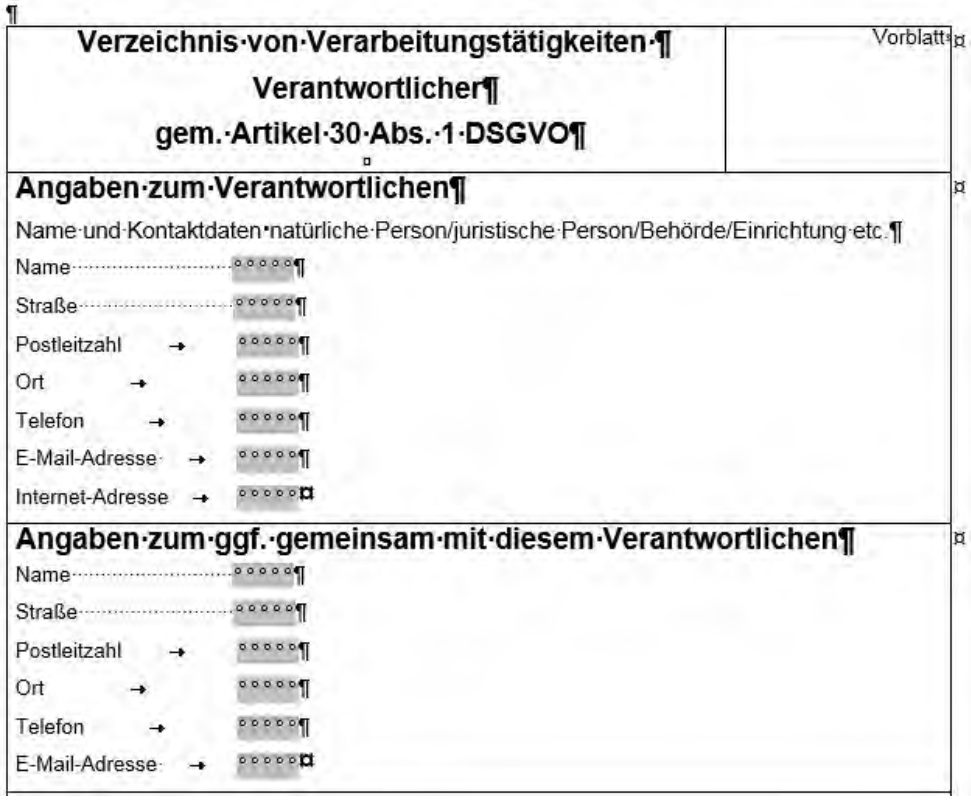
Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse
Internet-Adresse

Angaben zum ggf. gemeinsam mit diesem Verantwortlichen

Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse

Quelle: Bayerisches Landesamt für Datenschutzaufsicht



Verzeichnis von Verarbeitungstätigkeiten
Verantwortlicher
gem. Artikel 30 Abs. 1 DSGVO

Vorblatt

Angaben zum Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse
Internet-Adresse

Angaben zum ggf. gemeinsam mit diesem Verantwortlichen

Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse

Quelle: Hessischer Beauftragter für Datenschutz

Verarbeitungsverzeichnisse

Übersicht – Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO

Typische Verarbeitungstätigkeiten, die beim Betrieb eines Unternehmens stattfinden und aufzunehmen sind

- Beschaffung/Einkauf von Materialien mittels SAP-Tool
- Newsletter Tool
- Webseite, soweit personenbezogene Daten auch aus Kontaktformularen oder Kommentaren gespeichert werden
- Fotografien bei Veranstaltungen
- Personalaktenführung
- Lohn-, Gehalts- und Bezüge-Abrechnung
- Arbeitszeiterfassung
- Bewerbungsverfahren

Verarbeitungsverzeichnisse

Was müssen Unternehmen jetzt tun?

Verarbeitungsvoraussetzungen prüfen und aktuelles Verfahrensverzeichnis erstellen!

- Übersicht über alle Verarbeitungsvorgänge erstellen: Aktuelles Verzeichnis von Verarbeitungstätigkeiten
- Altes Verfahrensverzeichnis an neue Rechtslage anpassen
- Alte technisch-organisatorische Maßnahmen an neue IT-Schutzziele anpassen
- Rechtsgrundlagen der Datenverarbeitung auf Einschlägigkeit prüfen (lassen)

Technisch-organisatorische Maßnahmen

Übersicht – Sicherheit der Verarbeitung nach Art. 32 DS-GVO

Zielsetzung

Gewährleistung eines dem Risiko angemessenen Schutzniveaus

Umsetzung durch geeignete technische und organisatorische Maßnahmen, die getroffen werden

- Berücksichtigung des **Stands der Technik**
- **Implementierungskosten**
- **Art**, **Umfang**, **Umstände** und **Zwecke** der Verarbeitung
- **Eintrittswahrscheinlichkeit** und **Schwere** des Risikos

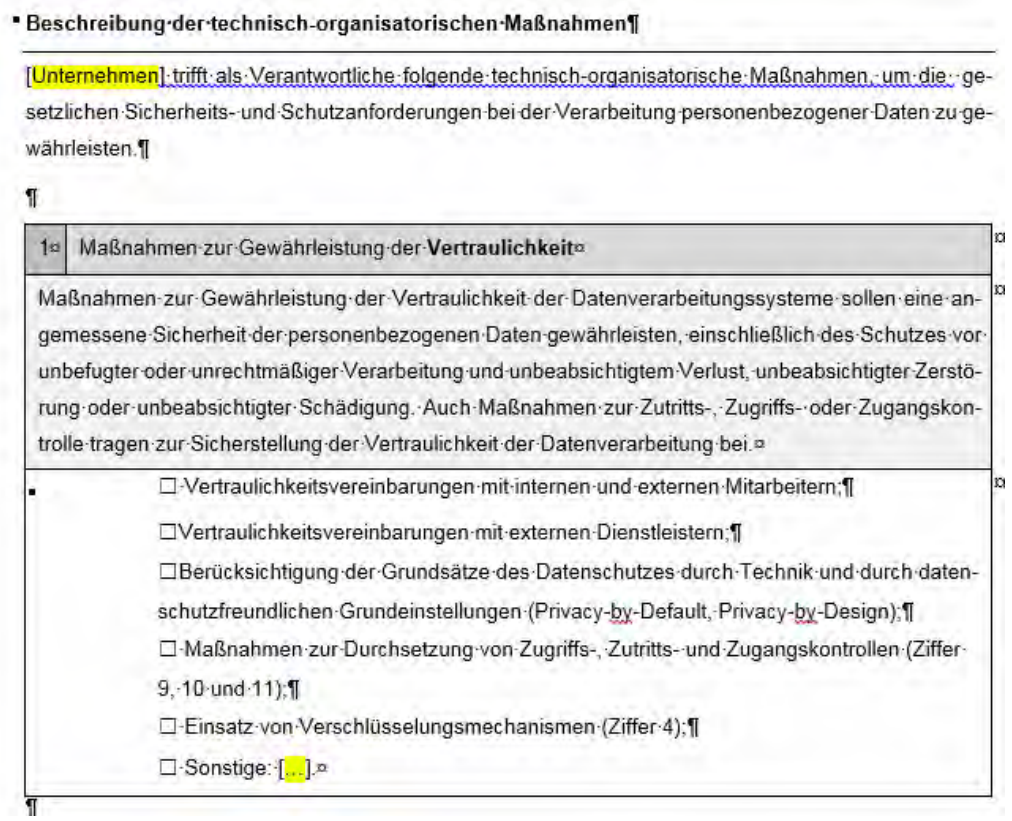
NEU: Verstoß ist bußgeldbewehrt (10 Mio. Euro / 2 % des Vorjahresumsatzes)!

Technisch-organisatorische Maßnahmen

Übersicht – Sicherheit der Verarbeitung nach Art. 32 DS-GVO

Einbeziehung klassischer IT-Schutzziele

- Pseudonymisierung und Verschlüsselung
- Vertraulichkeit
- Integrität
- Verfügbarkeit und Belastbarkeit der Systeme
- Verfügbarkeit der und Zugang zu den Daten
- Evaluierung der technischen und organisatorischen Maßnahmen



Beschreibung der technisch-organisatorischen Maßnahmen

[Unternehmen] trifft als Verantwortliche folgende technisch-organisatorische Maßnahmen, um die gesetzlichen Sicherheits- und Schutzanforderungen bei der Verarbeitung personenbezogener Daten zu gewährleisten.

1	Maßnahmen zur Gewährleistung der **Vertraulichkeit**
Maßnahmen zur Gewährleistung der Vertraulichkeit der Datenverarbeitungssysteme sollen eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Auch Maßnahmen zur Zutritts-, Zugriffs- oder Zugangskontrolle tragen zur Sicherstellung der Vertraulichkeit der Datenverarbeitung bei.	
☐ Vertraulichkeitsvereinbarungen mit internen und externen Mitarbeitern; ☐ Vertraulichkeitsvereinbarungen mit externen Dienstleistern; ☐ Berücksichtigung der Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundlichen Grundeinstellungen (Privacy-by-Default, Privacy-by-Design); ☐ Maßnahmen zur Durchsetzung von Zugriffs-, Zutritts- und Zugangskontrollen (Ziffer 9, 10 und 11); ☐ Einsatz von Verschlüsselungsmechanismen (Ziffer 4); ☐ Sonstige: [...].	

Musterdokument SKW Schwarz

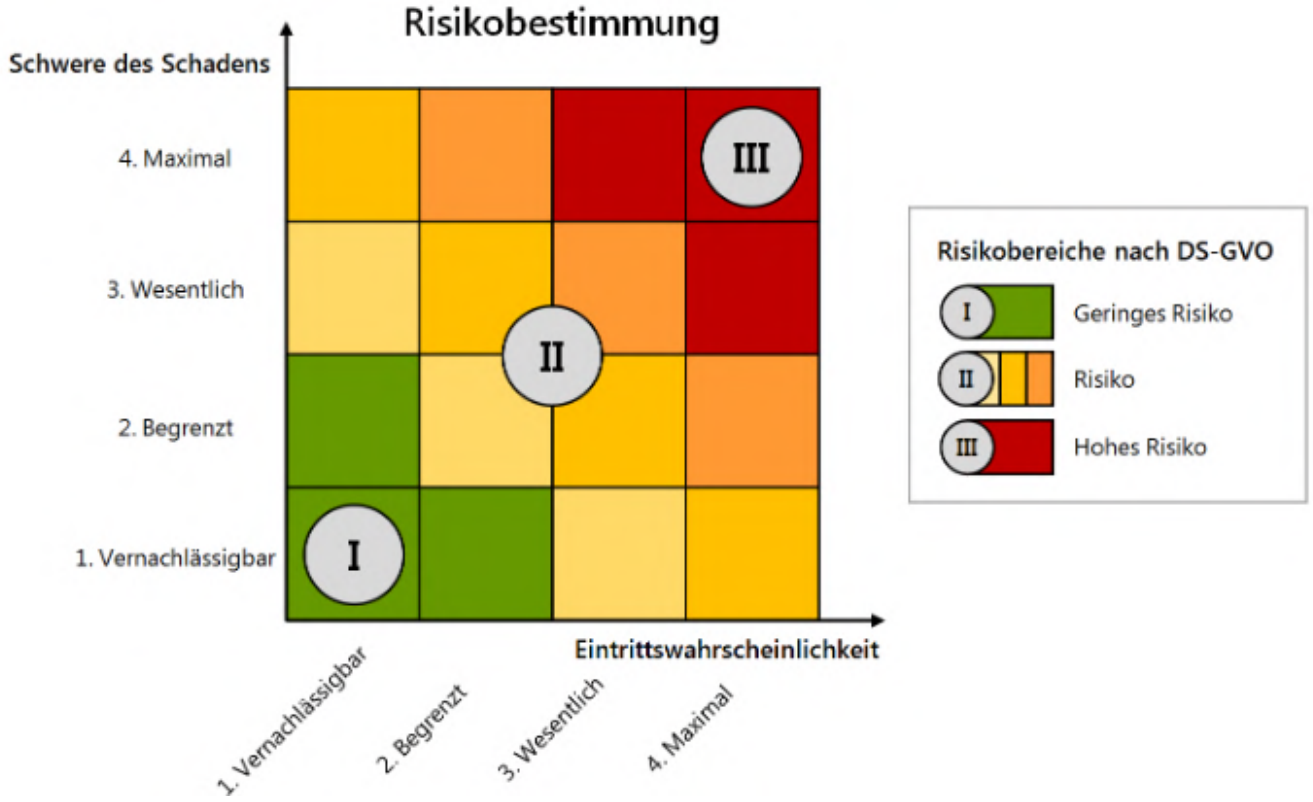
Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO

Übersicht

- Erfolgt durch den für die Verarbeitung Verantwortlichen (Art. 35 Abs. 1)
- Ist durchzuführen, wenn die Form der Verarbeitung „*aufgrund der Art, des Umfangs und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur* Folge“ hat
- Dokumentation der eingesetzten Abhilfemaßnahmen zur Eindämmung des Risikos, einschließlich Nachweisanforderungen
- Bei Verstoß: Sanktionsrahmen bis 10 Mio. Euro / 2 % des Vorjahresumsatzes

Datenschutz-Folgenabschätzung

Übersicht – Zu berücksichtigende Risiken nach Erwägungsgrund 75 der DS-GVO



Schwere des Risikos	
Vernachlässigbar	Kleine Unannehmlichkeiten
Begrenzt	Größere Unannehmlichkeiten
Wesentlich	Wesentliche Folgen
Maximal	Wesentliche und/oder irreversible Folgen

Eintrittswahrscheinlichkeit	
Vernachlässigbar	Fast unmöglich / nicht vorstellbar
Begrenzt	Mit gewissem Aufwand machbar (schwierig)
Wesentlich	Mit geringem Aufwand machbar
Maximal	Einfach

Zu berücksichtigende Risiken

- Identitätsdiebstahl
- Diskriminierung
- Finanzieller Verlust
- Rufschädigung
- Verlust der Vertraulichkeit bei Berufsgeheimnis
- Aufhebung der Pseudonymisierung
- Wirtschaftliche oder gesellschaftliche Nachteile
- Hinderung der Kontrolle der Betroffenen über eigene Daten
- Verarbeitung besonders schutzwürdiger Daten (Politik, Religion, Sexualleben, Gesundheit, etc.)

Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO

Positivlisten verschiedener Aufsichtsbehörden

– Nach Art. 35 Abs. 4 DS-GVO erstellen die Aufsichtsbehörden Listen für solche Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist
– Relevant für das Hotelgewerbe insbesondere: Automatisierte Auswertung von **Videoaufnahmen**; Einsatz von **RFID/NFC**; Betrieb von **Bewertungsportalen**, **Fraud Prevention-Systeme**

Bundesbeauftragte für Datenschutz und Informationsfreiheit

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Liste von Verarbeitungsvorgängen gemäß Artikel 35 Abs. 4 DSGVO

Rechtsgrundlage

Artikel 35 Absatz 4 der Datenschutz-Grundverordnung (DSGVO) verpflichtet die Aufsichtsbehörden, eine Liste von Verarbeitungsvorgängen zu erstellen, zu veröffentlichen und an den Europäischen Datenschutzausschuss zu übermitteln, für die in jedem Fall eine Datenschutz-Folgenabschätzung erforderlich ist, weil sie voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen.

Datenschutzkonferenz

DSK
DATENSCHUTZKONFERENZ

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
1	Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung natürlicher Personen, wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft: • Daten zu schutzbedürftigen Betroffenen • Systematische Überwachung • Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen • Bewerten oder Einstufen (Scoring) • Abgleichen oder Zusammenführen von Datensätzen • 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	Verwendung von biometrischen Systemen zur Zutrittskontrolle oder für Abrechnungszwecke.	Ein Unternehmen setzt flächendeckend Fingerabdrucksensoren zur Zutrittskontrolle für bestimmte Bereiche ein. Eine Schulkantine bietet den Schülern das „Bezahlen per Fingerabdruck“ an.

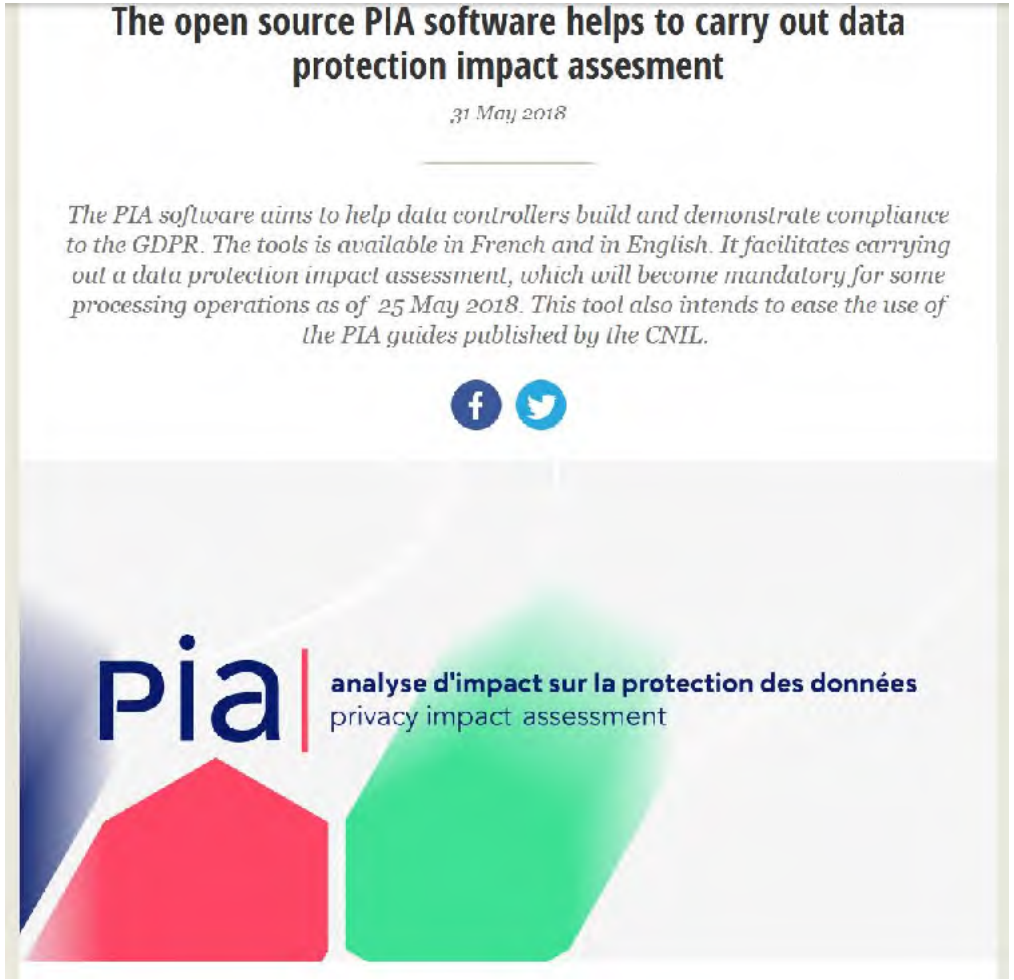
Datenschutz-Folgenabschätzung

Beispiel: Tool der Französischen Aufsichtsbehörde

Französische Aufsichtsbehörde bietet ein kostenloses Tool zu Durchführung einer DSFA/PIA an

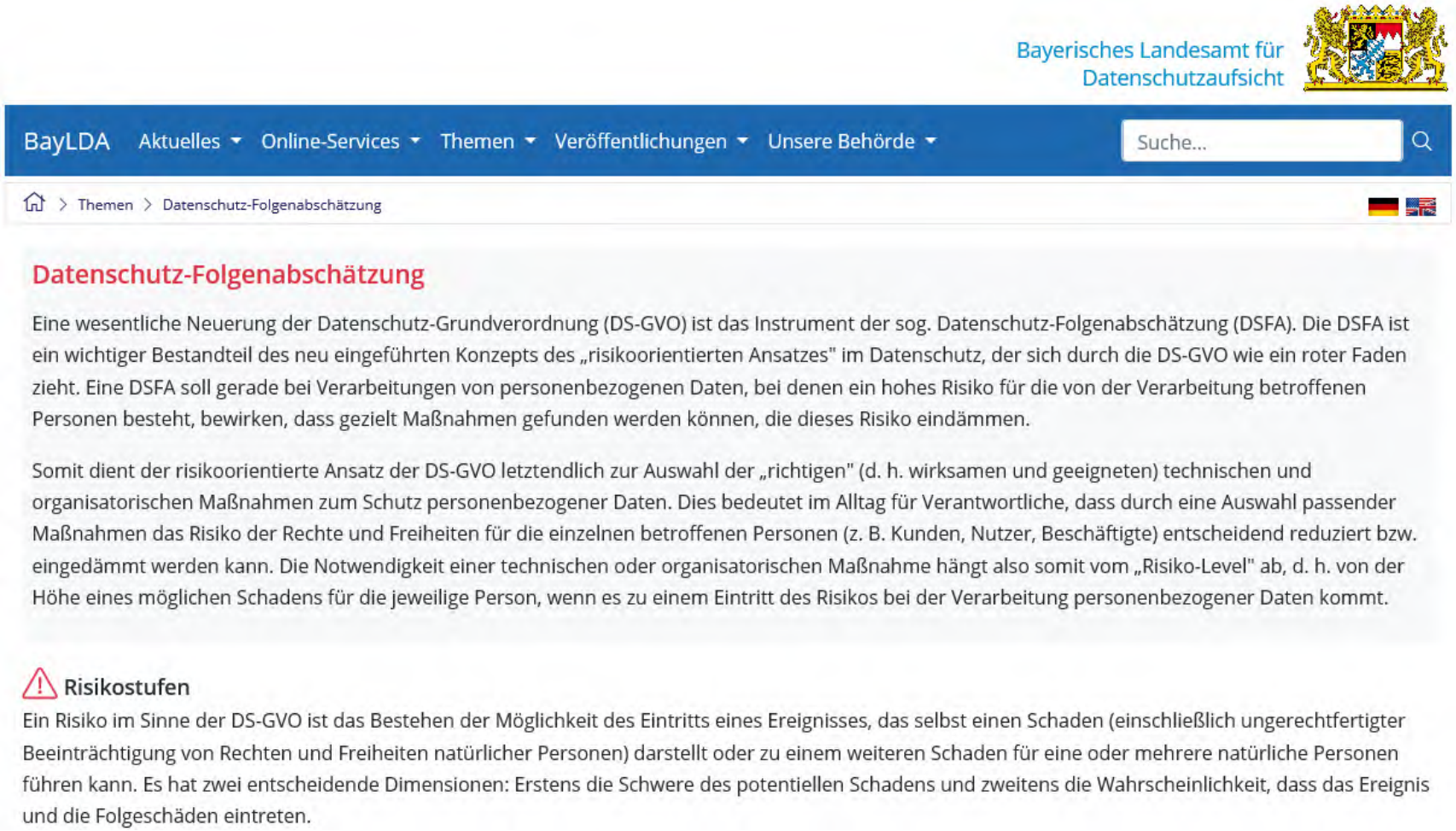
- Es besteht die Möglichkeit unternehmensspezifische Faktoren im Tool selbst zu integrieren
- Das Programm kann sowohl lokal auf einem PC (Windows, Mac, Linux) installiert werden, als auch web-basiert genutzt werden

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS



Datenschutz-Folgenabschätzung

Beispiel: Musterbeispiel LDA Bayern



Bayerisches Landesamt für Datenschutzaufsicht

BayLDA Aktuelles Online-Services Themen Veröffentlichungen Unsere Behörde Suche...

Themen > Datenschutz-Folgenabschätzung

Datenschutz-Folgenabschätzung

Eine wesentliche Neuerung der Datenschutz-Grundverordnung (DS-GVO) ist das Instrument der sog. Datenschutz-Folgenabschätzung (DSFA). Die DSFA ist ein wichtiger Bestandteil des neu eingeführten Konzepts des „risikoorientierten Ansatzes" im Datenschutz, der sich durch die DS-GVO wie ein roter Faden zieht. Eine DSFA soll gerade bei Verarbeitungen von personenbezogenen Daten, bei denen ein hohes Risiko für die von der Verarbeitung betroffenen Personen besteht, bewirken, dass gezielt Maßnahmen gefunden werden können, die dieses Risiko eindämmen.

Somit dient der risikoorientierte Ansatz der DS-GVO letztendlich zur Auswahl der „richtigen" (d. h. wirksamen und geeigneten) technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten. Dies bedeutet im Alltag für Verantwortliche, dass durch eine Auswahl passender Maßnahmen das Risiko der Rechte und Freiheiten für die einzelnen betroffenen Personen (z. B. Kunden, Nutzer, Beschäftigte) entscheidend reduziert bzw. eingedämmt werden kann. Die Notwendigkeit einer technischen oder organisatorischen Maßnahme hängt also somit vom „Risiko-Level" ab, d. h. von der Höhe eines möglichen Schadens für die jeweilige Person, wenn es zu einem Eintritt des Risikos bei der Verarbeitung personenbezogener Daten kommt.

Risikostufen

Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann. Es hat zwei entscheidende Dimensionen: Erstens die Schwere des potentiellen Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.

Datenschutz-Folgenabschätzung

Beispiel: Muster von SKW Schwarz (3-stufiges Vorgehen)

ID	Datenschutzrechtliche Risikobewertung / Datenschutzszenarien	Schadensmaß [1-5, 1=sehr niedrig / 5 = sehr hoch]	Eintrittswahrscheinlichkeit [0-5, 0=trifft nicht zu, keine / 1=sehr niedrig / 5 = sehr hoch]
	Wie schätzen Sie das Risiko im Hinblick auf die nachfolgenden Szenarien ein?		
D-1	Unbeabsichtigte/unrechtmäßige Vernichtung und/oder Verlust von personenbezogenen Daten		
D-2	Unbeabsichtigte/unrechtmäßige Veränderung von personenbezogenen Daten		
D-3	Unrechtmäßige Verarbeitung personenbezogener Daten durch Auftragsverarbeiter (Dienstleister)		
D-4	Unrechtmäßige Übermittlung an einen Dritten		
D-5	Zu Umfangreiche Datensammlung		
D-6	Reputationsschäden – z.B. unrechtmäßige Veröffentlichung personenbezogener Daten		
D-7	Kontrollverlust der betroffenen Person über ihre personenbezogenen Daten		
D-8	Unzureichende Information über Profiling oder Scoring an betroffene Person		
D-9	Unberechtigter Zugriff auf besondere Kategorien von Daten nach Artikel 9 DSGVO		
D-10	Datenabfluss/unberechtigter Zugriff durch erstmaligen Einsatz neuer Technologien		
D-11	Mögliche wesentliche prozessuale und/oder technischen Änderungen		
D-12	Zugriff durch unbefugte Dritte (u.a. Behörden, Dienstleister)		
D-13	Falsche Klassifikation/Rating des Kunden		
D-14	Zweckänderung (Überdehnung) ohne Information an die betroffene Person		
D-15	Schwächen in Datenqualität		
D-16	Hohe Anzahl Mitarbeiter mit Zugriff auf personenbezogene Daten		
D-17	Unzureichende Steuerung/Überwachung des Auftragsverarbeiters		
D-18	Auftragsverarbeitung in Drittstaaten		
D-19	Videoüberwachung öffentlicher Bereiche		
D-20	Unzureichende Datenschutz-Dokumentation		

Meldepflicht bei Datenschutzverstößen

Mehrteilige Regelung nach Art. 33 und 34 DS-GVO sowie Erwägungsgrund 59, 67 ff.

AUSLÖSER DER MELDEPFLICHT

„Verletzung des Schutzes personenbezogener Daten“, Art. 4 Abs. 9

→ **Risiko steigt und Meldepflichten stellen den Regelfall dar!**

→ **Achtung: Meldepflicht besteht auch für Auftragsverarbeiter gegenüber Kunden.**

ZWEISTUFIGE MELDEPFLICHT

Meldung an Aufsichtsbehörde innerhalb von **72 Stunden**, Art. 33

- Ist der **Regelfall**, außer es kommt „*voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten*“
- **Verzögerungen** sind gesondert zu begründen

→ **Grundsatz der Meldepflicht!**

Benachrichtigung der betroffenen Personen, Art. 34

- Meldepflicht, falls Wahrscheinlichkeit für hohes Risiko
- Stellt die **Ausnahme** dar

BEI VERSTOSS

Bis 10 Mio. Euro / 2 % des Vorjahresumsatzes

Meldepflicht bei Datenschutzverstößen

Übersicht

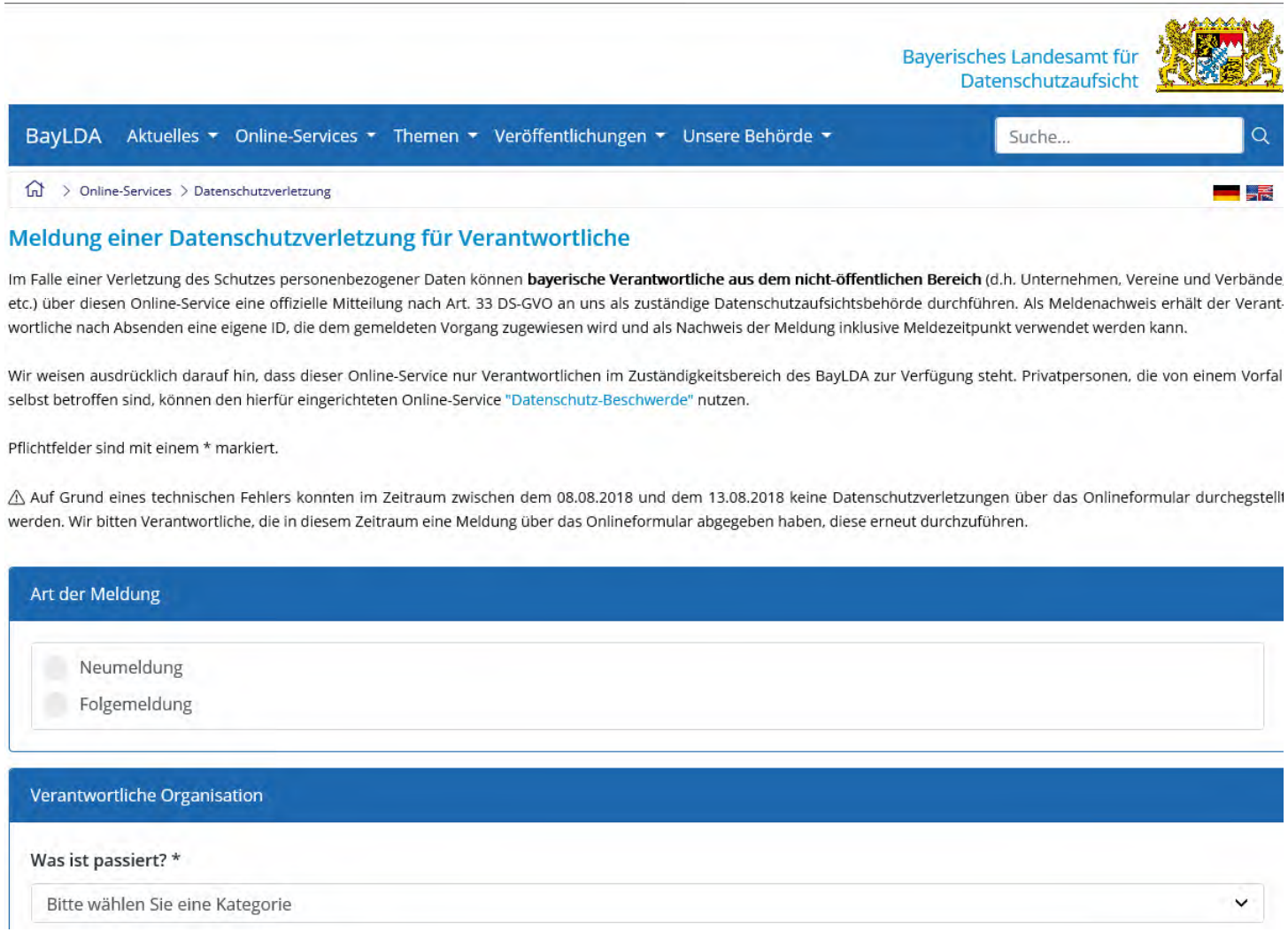
Was sind Datenschutzverletzungen?
– Insbesondere jegliche Vorgänge, durch unbefugten Dritten personenbezogene Daten zur Verfügung gestellt werden können
– Jeglicher Verlust mobiler Datenträger wie USB-Sticks oder mobile Festplatten, aber auch Smartphones oder Laptops
– Versehentliches Versenden von E-Mails an falsche Empfänger

Statistik des Bayerischen Landesamtes für Datenschutzaufsicht

BayLDA Statistik	2013	2014	2015	2016	2017	2018 (01.01-17.09)	2018	2018	Trend
						Summe	davon bis 25.Mai	davon seit 25.Mai	
Beratungen Vereine, Unternehmen	1733	1821	1850	2003	2974	6629	3834	2795	↑↑
Beratungen Privatpersonen	799	991	977	1065	1104	772	399	373	→
Beschwerden	925	953	1103	1424	1707	2229	731	1498	↑
Bußgeldverfahren	53	64	94	79	78	82	49	33	→
„Datenpannen“	32	21	28	85	150	1231	92	1139	↑↑↑

Meldepflicht bei Datenschutzverstößen

Onlineportal Landesdatenschutzaufsicht Bayern



Auftragsverarbeitung nach Art. 28 DS-GVO

Übersicht

Grundsatz der Privilegierung bleibt

– Auftragsverarbeiter ist kein Dritter i.S.d. Art. 4 Abs. 10 DS-GVO

Verantwortlicher für Verarbeitung bleibt verantwortlich

– Pflichtinhalte bei Beauftragung
– Angemessenheit der Schutzmaßnahmen
– Nachweis der ausreichenden Schutzmaßnahmen
– Einbindung von Subunternehmern nur bei einzelspezifischer oder genereller Erlaubnis

NEU: Geänderte inhaltliche Anforderungen an Vereinbarung
NEU: Gemeinsame Haftung (Art. 28) des Auftraggebers und des Auftragnehmers

Bei Verstoß: Sanktionsrahmen bis 10 Mio. Euro / 2 % des Vorjahresumsatzes

– Bußgelder sowohl gegen Verantwortlichen als auch gegen Auftragsverarbeiter möglich
– Gemeinsame Haftung für Schadensersatzansprüche nach Art. 82 DS-GVO

Auftragsverarbeitung nach Art. 28 DS-GVO

Übersicht

Wichtigste Pflichten des Auftragsverarbeiters

- Zweckbindung und Weisungsgebundenheit
- Verpflichtung zur Vertraulichkeit (vormals Datengeheimnis)
- Einhaltung von angemessenen technisch-organisatorischen Maßnahmen
- Unterauftragsverhältnisse werden datenschutzrechtlich auch abgesichert
- Unterstützung des Verantwortlichen bei der Erfüllung seiner Pflichten nach der DS-GVO
- Rückgabe überlassener Datenträger und Löschpflichten
- Meldung von Unregelmäßigkeiten und Verstößen

NEU: Der Auftragsverarbeiter ist auch Bußgeldadressat und haftet gegenüber der betroffenen Person auf Schadensersatz

Pflichtinhalte bei Beauftragung

- Pflichtinhalte eines AV-Vertrags richten sich nach Art. 28 Abs. 3 DS-GVO
- Dazu gehören unter anderem folgende Angaben: Gegenstand und Dauer der Datenverarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien personenbezogener Daten, Pflichten und Rechte des Verantwortlichen, Pflichten und Rechte des Auftragsverarbeiters

Auftragsverarbeitung nach Art. 28 DS-GVO

FAQ-Dokument des Bayerischen Landesamtes für Datenschutz

FAQ zur DS-GVO

Bayerisches Landesamt für Datenschutzaufsicht

Stichworte	Auftragsverarbeitung, Abgrenzung
Norm	Art. 4 Nr. 8 und Art. 28 DS-GVO
Frage	Was ist Auftragsverarbeitung und was nicht?
Antwort	Auftragsverarbeitung im datenschutzrechtlichen Sinne liegt nur in Fällen vor, in denen eine Stelle von einer anderen Stelle im Schwerpunkt mit der Verarbeitung personenbezogener Daten beauftragt wird. Die Beauftragung mit fachlichen Dienstleistungen anderer Art, d. h., mit Dienstleistungen, bei denen nicht die Datenverarbeitung im Vordergrund steht bzw. bei denen die Datenverarbeitung nicht zumindest einen wichtigen (Kern-)Bestandteil ausmacht, stellt keine Auftragsverarbeitung im datenschutzrechtlichen Sinne dar.

Hiernach ist Auftragsverarbeitung insbesondere:

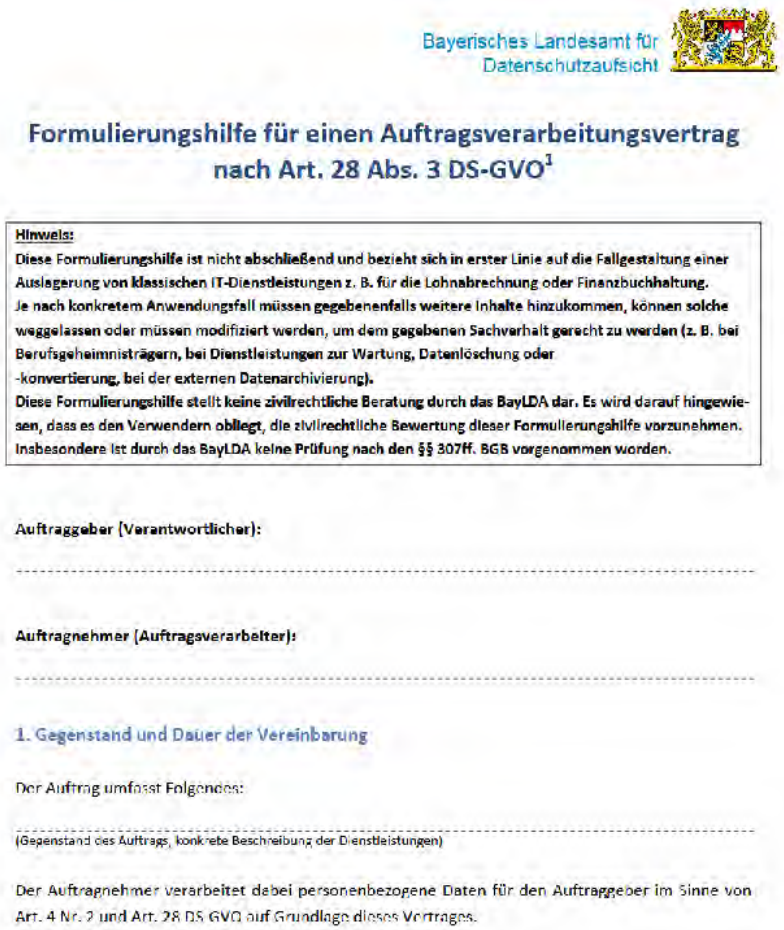
- Externe Lohn- und Gehaltsabrechnung
- Outsourcing im Rahmen der Nutzung von Cloud-Diensten
- Adressverarbeitung in Lettershops
- Auslagerung der E-Mail-Verwaltung
- Datenträgerentsorgung durch Fachunternehmen
- IT-Wartungsarbeiten (Fernwartung, externer Support)
- Sicherheitsdienste, die Gäste- oder Zuliefererdaten erheben

Hiernach ist Auftragsverarbeitung insbesondere nicht:

- Tätigkeiten von Berufsgeheimnisträgern (Rechtsanwälte, Steuerberater)
- Postdienste
- Tätigkeiten von Tourismus-Büros
- Bankinstitute
- Hersteller und Großhändler bei regelmäßiger Warenlieferung
- TK-Dienstleistungen
- Handelsvertreter

Auftragsverarbeitung nach Art. 28 DS-GVO

Musterdokumente der Aufsichtsbehörden Bayern und Hessen



Bayerisches Landesamt für Datenschutzaufsicht

Formulierungshilfe für einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO[1]

Hinweis:
Diese Formulierungshilfe ist nicht abschließend und bezieht sich in erster Linie auf die Fallgestaltung einer Auslagerung von klassischen IT-Dienstleistungen z. B. für die Lohnabrechnung oder Finanzbuchhaltung. Je nach konkretem Anwendungsfall müssen gegebenenfalls weitere Inhalte hinzukommen, können solche weggelassen oder müssen modifiziert werden, um dem gegebenen Sachverhalt gerecht zu werden (z. B. bei Berufsgeheimnisträgern, bei Dienstleistungen zur Wartung, Datenlöschung oder -konvertierung, bei der externen Datenarchivierung).
Diese Formulierungshilfe stellt keine zivilrechtliche Beratung durch das BayLDA dar. Es wird darauf hingewiesen, dass es den Verwendern obliegt, die zivilrechtliche Bewertung dieser Formulierungshilfe vorzunehmen. Insbesondere ist durch das BayLDA keine Prüfung nach den §§ 307ff. BGB vorgenommen worden.

Auftraggeber (Verantwortlicher):

Auftragnehmer (Auftragsverarbeiter):

---

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

(Gegenstand des Auftrags, konkrete Beschreibung der Dienstleistungen)

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Formulierungshilfe für einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO[1],

Auftraggeber (Verantwortlicher):

Auftragnehmer (Auftragsverarbeiter):

---

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

(Gegenstand des Auftrags, konkrete Beschreibung der Dienstleistungen)

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Datentransfer in Länder außerhalb der EU / des EWR

Übersicht

Entscheidungen der Kommission über die Angemessenheit des Schutzes personenbezogener Daten in Drittländer	US Privacy Shield	EU-Standardvertragsklauseln Art 46 DS-GVO	Binding Corporate Rules (BCR) Art 47 DS-DGVO
Die Kommission hat bislang folgende Länder anerkannt, die einen angemessenen Schutz bieten: • Andorra • Argentinien • Kanada (kommerzielle Organisationen) • Färöer Inseln • Guernsey • Israel, Isle Of Man • Jersey • Neuseeland • Schweiz • Uruguay	• Unternehmen müssen interne Datenschutzrichtlinien haben und diese veröffentlichen. • US-Unternehmen unterliegen den Weisungen des Handels-ministeriums und der europäischen Datenschutz-aufsichtsbehörden. • Betroffenenrechte in den USA werden gestärkt. • Geheimdienste dürfen nicht mehr massenhaft auf Daten zugreifen. • Aktuell 2.517 Gesellschaften gelistet.	• Festgeschriebenes Vertragswerk der EU-Kommission. • Keinerlei Änderungen erlaubt (kein Punkt, kein Komma)	• Verbindliche interne Datenschutzvorschriften bei einer Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben. • Aufwändig und teuer für Unternehmen (Zertifizierung)

Datentransfer in Länder außerhalb der EU / des EWR

Hohe Praxisrelevanz: EU Standardvertragsklauseln

L 39/10 DE Amtsblatt der Europäischen Union 12.2.2010

ANHANG

STANDARDVERTRAGSKLAUSELN (AUFTRAGSVERARBEITER)

gemäß Artikel 26 Absatz 2 der Richtlinie 95/46/EG für die Übermittlung personenbezogener Daten an Auftragsverarbeiter, die in Drittländern niedergelassen sind, in denen kein angemessenes Schutzniveau gewährleistet ist

Bezeichnung der Organisation (Datenexporteur): .....

Anschrift: .....

Tel. ..... Fax ..... E-Mail: .....

Weitere Angaben zur Identifizierung der Organisation

.....

(„Datenexporteur")

und

Bezeichnung der Organisation (Datenimporteur): .....

Anschrift: .....

Tel.: Fax: E-Mail:

Weitere Angaben zur Identifizierung der Organisation:

.....

(„Datenimporteur")

(die „Partei", wenn eine dieser Organisationen gemeint ist, die „Parteien", wenn beide gemeint sind)

VEREINBAREN folgende Vertragsklauseln („Klauseln"), um angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen bei der Übermittlung der in Anhang 1 zu diesen Vertragsklauseln spezifizierten personenbezogenen Daten vom Datenexporteur an den Datenimporteur zu bieten.

Klausel 1

– Nutzung ohne inhaltliche Veränderung
– Barrierefrei im Internet herunterladbar
– In allen Sprachen der Mitgliedsstaaten der EU / des EWR

2010/87/: Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (Bekannt gegeben unter Aktenzeichen K(2010) 593) (Text von Bedeutung für den EWR)

OJ L 39, 12.2.2010, p. 5–18 (BG, ES, CS, DA, DE, ET, EL, EN, FR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
Special edition in Croatian: Chapter 13 Volume 052 P. 250 - 263

ELI: http://data.europa.eu/eli/dec/2010/87/oj

Languages, formats and link to OJ

	BG	ES	CS	DA	DE	ET	EL	EN	FR	GA	HR	IT	LV	LT	HU	MT	NL	PL	PT	RO	SK	SL	FI	SV
HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML		HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML
PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF		PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF
Official Journal																								

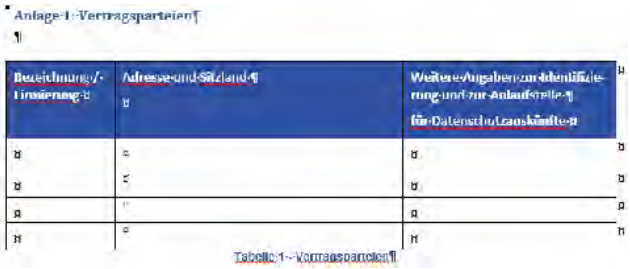
Datentransfer in Länder außerhalb der EU / des EWR

IT-Rahmenvertragslösung bei komplexen Sachverhalten

IT-Rahmenvertrag für EU-Standarddatenschutzklauseln

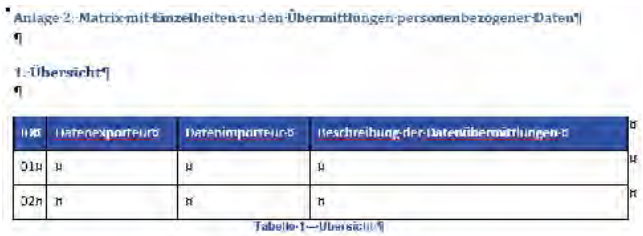
zwischen

den in der **Anlage 1** aufgeführten Vertragsparteien.



Anlage 1: Vertragsparteien

Anlage 1: Vertragsparteien



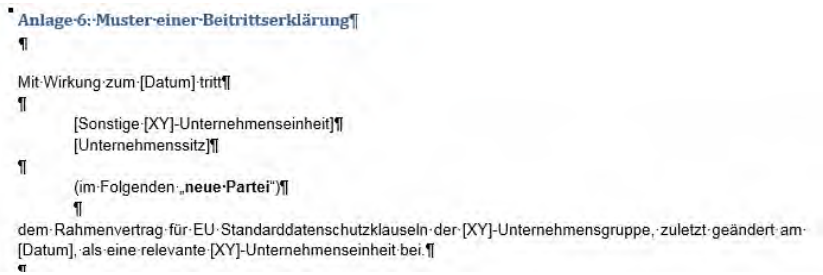
Anlage 2: Matrix mit Einzelheiten zu den Übermittlungen personenbezogener Daten

Anlage 2: Verarbeitungsmatrix

ANHANG

STANDARDVERTRAGSKLAUSELN (AUFTRAGSVERARBEITER)

Anlage 3: EU Standardvertrag



Anlage 6: Muster einer Beitrittserklärung

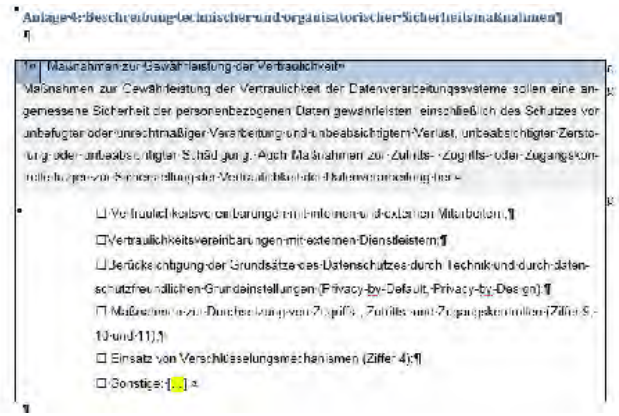
Mit Wirkung zum [Datum] tritt

[Sonstige [XY]-Unternehmenseinheit]
[Unternehmenssitz]

(im Folgenden „**neue Partei**")

dem Rahmenvertrag für EU Standarddatenschutzklauseln der [XY]-Unternehmensgruppe, zuletzt geändert am [Datum], als eine relevante [XY]-Unternehmenseinheit bei.

Anlage 6: Beitrittserklärung



Anlage 4: Beschreibung technischer und organisatorischer Sicherheitsmaßnahmen

Maßnahmen zur Gewährleistung der Vertraulichkeit

Maßnahmen zur Gewährleistung der Vertraulichkeit der Datenverarbeitungssysteme sollen eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Auch Maßnahmen zur Zutritts-, Zugriffs- oder Zugangskontrolle, sowie zur Sicherstellung der Vertraulichkeit der Datenverarbeitung (siehe S. 10 und 11).

- ☐ Vertraulichkeitsvereinbarungen mit internen und externen Mitarbeitern
- ☐ Vertraulichkeitsvereinbarungen mit externen Dienstleistern
- ☐ Berücksichtigung der Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundlichen Grundeinstellungen (Privacy-by-Default, Privacy-by-Design)
- ☐ Maßnahmen zur Durchsetzung von Zugriffs-, Zutritts- und Zugangskontrollen (Ziffer 8 - 10 und 11)
- ☐ Einsatz von Verschlüsselungsmechanismen (Ziffer 4)
- ☐ Sonstige:

Anlage 4: ToM

Anlage 5: Außerkraft tretende Verträge zwischen [...] Unternehmenseinheiten

Anlage 5: Obsolete Vereinbarungen

Datenschutzbeauftragter

Übersicht

Bestellpflicht und Anforderungen an die Bestellung

- **Bestellpflicht** nach der DS-GVO (Art. 37 Abs. 1 DS-GVO)
- Besondere Regelung in§ 38 BDSG-neu; hiernach Pflicht bei **10 Angestellten**, die regelmäßig mit personenbezogenen Daten umgehen (erfasst insbesondere Rezeption, Buchhaltung, Personalabteilung)
- **Qualifikation** und persönliche Voraussetzungen des DSB
  - berufliche Qualifikation und Fachwissen auf dem Gebiet des Datenschutzrechts
  - Vermeidung von Interessenkonflikten
- Pflicht zur Veröffentlichung der Kontaktdaten des DSB und **Mitteilung** dieser an die **Datenschutz-Aufsichtsbehörde** (Art. 37 Abs. 7 DS-GVO)

Stellung des Datenschutzbeauftragten

- **Unabhängigkeit** von fachlichen Weisungen und Berichtsweg zur höchsten Managementebene
- **Abberufungsschutz**, Benachteiligungsverbot und Sonderkündigungsschutz
- Einbindung, Unterstützung und Fortbildung des DSB

Der Datenschutzbeauftragte hat unter anderem folgende Aufgaben, Art. 38 DS-GVO

- **Unterrichtung** und Beratung bei datenschutzrechtlichen Themen
- **Überwachung** der Einhaltung des Datenschutzes
- **Zusammenarbeit** mit der Datenschutz-Aufsichtsbehörde

Datenschutzbeauftragter

Rechtsfolgen bei Verstoß und To Do‘s

Rechtsfolgen bei Verstoß

Verletzungen der Vorschriften zum Datenschutzbeauftragten (wie Nicht-Benennung, unzureichende Unterstützung oder Benachteiligung des DSB usw.) sind nach Art. 83 Abs. 4 lit. a DS-GVO mit einer Geldbuße in Höhe von bis zu 10 Mio. Euro oder 2% des weltweit erzielten Jahresumsatzes bedroht.

Vorgehensweise

- Prüfung, ob die **Pflicht** zur Benennung eines DSB **besteht**
- Entscheidung, ob ein **betrieblicher** oder **externer** DSB bestellt werden soll
- Anpassung der **Bestellurkunde** eines schon bestellten DSB an die DS-GVO
- Sicherstellung, dass der DSB tatsächlich frühzeitig in allen mit dem Datenschutz zusammenhängenden Fragen eingebunden wird
- **Meldung Kontaktdaten** an zuständige **Datenschutzaufsichtsbehörde** sowie **Aufnahme Kontaktdaten** bei **Datenschutzhinweisen**

04

Stellungnahmen der Aufsichtsbehörden zur Umsetzung der DS-GVO

Stellungnahmen von Aufsichtsbehörden

Datenschutzkonferenz - DSK

Kurzpapiere zu diversen Themen der Datenschutz-Grundverordnung

Die Datenschutzkonferenz (DSK) veröffentlich seit Juli 2017 Auslegungshilfen zur Datenschutz-Grundverordnung (DS-GVO). In diesen Kurzpapieren werden unter den deutschen Aufsichtsbehörden abgestimmte einheitliche Sichtweisen zu verschiedenen Kernthemen der DS-GVO wiedergegeben. Die in den Papieren enthaltenen Auffassungen stehen unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung durch den Europäischen Datenschutzausschuss.

Die Kurzpapiere des BayLDA, die bereits seit Juni 2016 in regelmäßigen Abständen erschienen sind, können ebenso heruntergeladen werden.

DSK-Kurzpapiere zur DS-GVO:

1. Verzeichnis von Verarbeitungstätigkeiten
2. Aufsichtsbefugnisse/Sanktionen
3. Verarbeitung personenbezogener Daten für Werbung
4. Datenübermittlung in Drittländer
5. Datenschutz-Folgenabschätzung
6. Auskunftsrecht
7. Marktortprinzip
8. Maßnahmenplan
9. Zertifizierung
10. Informationspflichten bei Dritt- und Direkterhebung
11. Recht auf Vergessenwerden
12. Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern
13. Auftragsverarbeitung
14. Beschäftigtendatenschutz
15. Videoüberwachung
16. Gemeinsam für die Verarbeitung Verantwortliche
17. Besondere Kategorien personenbezogener Daten

https://www.datenschutzkonferenz-online.de/

Stellungnahmen von Aufsichtsbehörden

Bayerisches Amt für Landesdatenschutzaufsicht

Kurzpapiere zu diversen Themen der Datenschutz-Grundverordnung

BayLDA-Kurzpapiere zur DS-GVO:

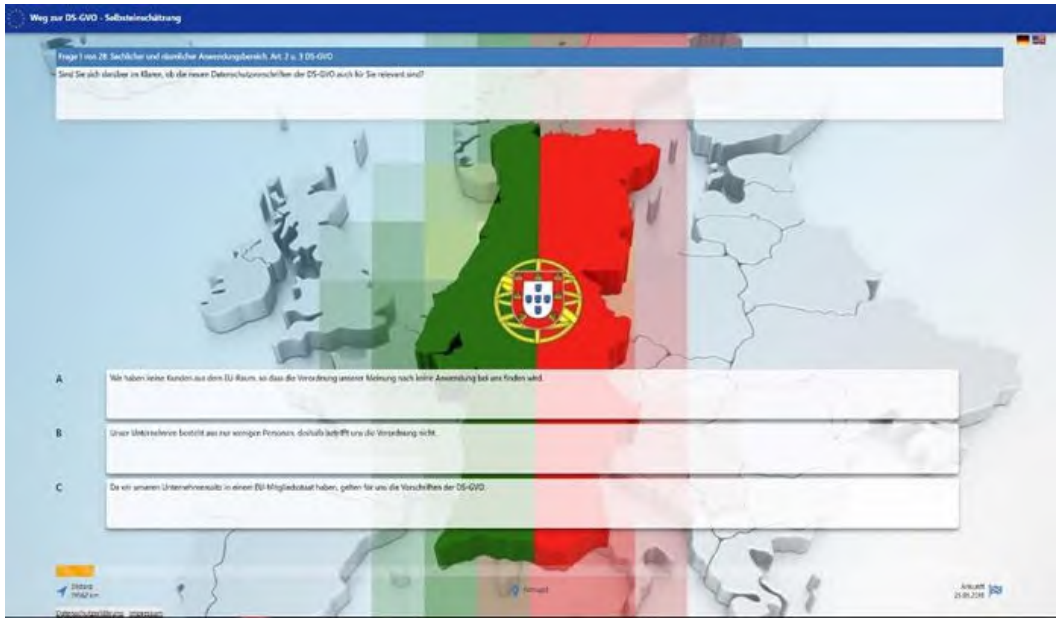
1. Veröffentlichung zum Art. 32 DS-GVO - Sicherheit der Verarbeitung
2. Art. 42 DS-GVO - Zertifizierung
3. *Videoüberwachung - Ersetzt durch DSK-Kurzpapier Nr. 15*
4. Recht auf Löschung ("Vergessenwerden") - Art. 17 DS-GVO
5. *Verzeichnis von Verarbeitungstätigkeiten - Ersetzt durch DSK-Kurzpapier Nr. 1*
6. Besondere Kategorien personenbezogener Daten - Art. 9 DS-GVO
7. *Sanktionen - Ersetzt durch DSK-Kurzpapier Nr. 2*
8. Umgang mit Datenpannen - Art. 33 und 34 DS-GVO
9. Einwilligungen nach der DS-GVO
10. Auftragsverarbeitung nach der DS-GVO
11. *Datenübermittlung in Drittländer - DSK-Kurzpapier Nr. 4.*
12. *Werbung - Ersetzt durch DSK-Kurzpapier Nr. 3*
13. One Stop Shop
14. Amtshilfe und gemeinsame Maßnahmen der Aufsichtsbehörden
15. Einwilligung eines Kindes
16. *Auskunftsrecht - Ersetzt durch DSK-Kurzpapier Nr. 6*
17. Verhaltensregeln - Art. 40 DS-GVO
18. *Datenschutz-Folgenabschätzung - Ersetzt durch DSK-Kurzpapier Nr. 5*
19. *Der Datenschutzbeauftragte (DSB) - Art. 37 bis 39 DS-GVO - Ersetzt durch DSK-Kurzpapier Nr. 12*
20. *Beschäftigtendatenschutz - Ersetzt durch DSK-Kurzpapier Nr. 14*

https://www.lda.bayern.de/

Stellungnahmen von Aufsichtsbehörden

Bayerisches Amt für Landesdatenschutzaufsicht

Tool zur DS-GVO Selbsteinschätzung sowie Fragebogen zur Umsetzung der DS-GVO



Fragebogen zur Umsetzung der DS-GVO zum 25. Mai 2018

Unternehmen/Verantwortliche Stelle	Eingangsstempel BayLDA

I. Struktur und Verantwortlichkeit im Unternehmen	
1.	▪ Gibt es das Bewusstsein im Unternehmen, dass Datenschutz Chefsache ist, beispielsweise durch ▪ Vorhandensein einer Datenschutzleitlinie ▪ Beschreibung der Datenschutzziele ▪ Regelung der Verantwortlichkeiten ▪ Bewusstsein über Datenschutzrisiken ▪ Transparenz über Zielkonflikte (z.B. zwischen Marketing- und Rechtsabteilung)
2.	▪ Verfügt Ihr Unternehmen über einen betrieblichen Datenschutzbeauftragten? ▪ Wenn nein, warum nicht? ▪ Wenn ja, ist geklärt, wann er von wem einzubeziehen ist? ▪ Wenn ja, ist er schon gem. Art. 37 Abs. 8 DS-GVO der zuständigen Aufsichtsbehörde gemeldet?
II. Übersicht über Verarbeitungen	
1.	▪ Haben Sie ein Verzeichnis Ihrer Verarbeitungstätigkeiten gem. Art. 30 DS-GVO? ▪ Wenn nein, warum nicht? Ist das dokumentiert? ▪ Wie haben Sie sichergestellt, dass datenschutzrechtliche Belange bei Beginn oder Änderung eines jeden Prozesses in Ihrem Unternehmen Berücksichtigung finden (Privacy by Design –Art. 25 DS-GVO)?
III. Einbindung Externer	
1.	▪ Haben Sie Externe zur Erledigung Ihrer Arbeiten (Auftragsverarbeiter) eingebunden? ▪ Wenn ja, haben Sie eine Übersicht über die Auftragsverarbeiter? ▪ Wenn ja, haben Sie mit allen Ihren Auftragsverarbeitern die erforderlichen Vereinbarungen mit dem Mindestinhalt nach Art. 28 Abs. 3 DS-GVO abgeschlossen?

05

Brennpunkte zum aktuellen Datenschutzrecht

Umgang mit Social-Media Fanpages und Messenger-Diensten

Fanpages auf Social Media Plattformen

- EuGH bestätigt gemeinsame Verantwortung i.S.v. Art. 26 DS-GVO von Facebook und Fanpage-Betreibern
- Entschließung der DSK vom 6. Juni 2018 zur Fanpage-Problematik
  - Wer eine Fanpage besucht, muss transparent und in verständlicher Form darüber informiert werden, welche Daten zu welchen Zwecken durch Facebook und den Fanpage-Betreiber verarbeitet werden.
  - Betreiber von Fanpages sollten sich selbst versichern, dass Facebook ihnen die Informationen zur Verfügung stellt, die zur Erfüllung der Informationspflichten nach Art. 13, 14 DS-GVO benötigt werden.
  - Für die Bereiche der gemeinsamen Verantwortung von Facebook und Fanpage-Betreibern ist in einer Vereinbarung festzulegen, wer von ihnen welche Verpflichtung der DS-GVO erfüllt.
  - Die Nutzung von Fanpages verstößt gegen die DS-GVO, soweit Facebook kein datenschutzkonformes Produkt anbietet.

Umgang mit Social-Media Fanpages und Messenger-Diensten

Umgang mit Messenger-Apps auf mobilen Dienstgeräten

- Datenschutzrechtliche Zulässigkeit des Einsatzes von Messenger-Diensten
  - Problem: Datenübermittlung an den Anbieter und umfassende Verarbeitung personenbezogener Daten
    - Adressbuchvergleich bei Installation der App (sämtliche Kontaktinformationen werden automatisch übertragen)
    - Umfassende Verarbeitung personenbezogener Daten (Messungen, Analyse der Nutzung und Verarbeitung von Metadaten)
  - Folge: Abmahnungsgefahr und ggf. Schadensersatzansprüche
- Aktuelle Rechtsprechung: Einsatz ohne Einwilligung unzulässig (AG Bad Hersfeld, Az.: F 120/17 EASO)
- Meinungsbild der Datenschutz-Aufsichtsbehörden: Einsatz ohne Einwilligung unzulässig
  - Merkblatt des LfD Niedersachsen zur Nutzung von „WhatsApp“ in Unternehmen (Die Nutzung von WhatsApp verstößt insbesondere wegen des Adressabgleichs gegen Art. 5 Abs. 1 lit. c und gegen Art. 25 Abs. 1 DS-GVO)

Umgang mit Social-Media Fanpages und Messenger-Diensten

Umgang mit Messenger-Apps auf Diensthandys

- Lösungsansätze
  - Container-Lösung bzw. Mobile Device Management (kein Adressbuchabgleich von Daten, die sich außerhalb des „Containers“ befinden)
  - Nutzung von einem Mobilgerät, welches nur Kontaktdaten von Geschäftspartnern enthält, die ihrerseits auch den entsprechenden Dienst (z.B. WhatsApp) nutzen
  - Einwilligungen von sämtlichen in den Adressbuch enthaltenen Kontakten einholen, die den Dienst nicht nutzen
  - Datenschutzkonforme Alternativen von WhatsApp und Facebook Messenger suchen (z.B. Wire, Hoccer, Threema)

Umgang mit Social-Media Fanpages und Messenger-Diensten

Like-Buttons und Plugins und deren Implementierung auf der Webseite

- Umfassende Aufklärung über die Datenverarbeitung im Rahmen der Datenschutzerklärung der Webseite erforderlich (Art. 13, 14 DS-GVO)
  - Differenzierung zwischen der Einbindung von externen Links, Like-Buttons und Plugins
  - Erfüllung der Informationspflichten nach Art. 13, 14 DS-GVO
- Sicherstellung, dass keine personenbezogenen Daten (z.B. IP-Adresse) automatisch an die jeweilige Social-Media-Plattform übermittelt werden
  - Zwei-Klick-Lösung
  - Shariff-Lösung

Bsp. Zwei-Klick-Lösung

SKW
Schwarz
Rechtsanwälte

Vielen Dank

für Ihre Aufmerksamkeit

Dr. Oliver Hornung
Partner

SKW Schwarz
Moerfelder Landstrasse 117
60598 Frankfurt am Main, Germany
T +49 (0) 69 63 00 01-65
F +49 (0) 69 63 00 01-11
E o.hornung@skwschwarz.de