EDV Sachverständigen- und
Datenschutzbüro Michael J. Schüssler
Anerkannter EDV Sachverständiger
gemäss DSGSVO (ULD),
Schiedsgutachter, Wirtschafts-
informatiker, externer
Datenschutzbeauftragter & zert.
PECB ISO/IEC 27001 Lead Auditor
Kolpingstrasse 3
63739 Aschaffenburg
Email: info@svb-ms.de
Tel.: 06021 / 439 18 45
Mobil: 0179 / 49 68 941
www.datenschutz4you-aschaffenburg.de

Herzlich Willkommen zum Seminar „Betrieblicher Datenschutzbeauftragter“ gemäß DS-GVO & BDSG(neu)

Ihr Referent: Wirtschaftsinformatiker Michael J. Schüssler
EDV Sachverständigen- und Datenschutzbüro Michael J. Schüssler
Wirtschaftsinformatiker, Schiedsgutachter, anerkannter EDV-Sachverständiger (ULD), externer Datenschutzbeauftragter gemäß § 4f Abs. 2 S. 1 BDSG. ISO/IEC 27001 Foundation zert. und zertifizierter PECB ISO 27001 Lead Auditor.

Datenschutz ist ein spannendes Thema welches auch Ihre Persönlichkeitsrechte betrifft!

Informationelle Selbstbestimmung

Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit…
(GG Art. 2 Abs. 1)

Die DS-GVO und das BDSG(neu)

Art. 1 DS-GVO Gegenstand und Ziele

Abs. 1 Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

Abs. 2 Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und **insbesondere deren Recht auf Schutz personenbezogener Daten**.

Abs. 3 Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung pbD weder eingeschränkt noch verboten werden.

Sicht- und Stichtag 25Mai 2018

§ 1 BDSG (neu) Anwendungsbereich des Gesetzes

Abs. 1 Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,

2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie

a) Bundesrecht ausführen oder

b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

Für nichtöffentliche Stellen (AG, GmbH, Vereine…) gilt dieses Gesetz für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung pbD, die in einem **Dateisystem gespeichert** sind oder gespeichert werden sollen, es sei denn, die Verarbeitung durch natürliche Personen erfolgt zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten. Andere Rechtsvorschriften des Bundes über den Datenschutz gehen den Vorschriften dieses Gesetzes vor (**Subsidaritätsprinzip**).

Rechtsgrundlagen und Meilensteine im Datenschutz

Die Würde des Menschen ist unantastbar…
(GG Art. 1 Abs. 1)

Allgemeine Erklärung der Menschenrechte (UNO - 1948)

Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit…(GG Art. 2 Abs. 1)

1. Das Grundrecht auf informationelle Selbstbestimmung (BVerfG, 19 . .)
2. Europäische Datenschutzrichtlinie 95/ . ./ . . (19 . .)
3. Bundesdatenschutzgesetz (Novelle III, 2 . . .)
4. **Die EU-Datenschutz-Grund . . . . . (DS- . . ., 25.Mai 2018)**
5. **Bundesdatenschutzgesetz (BDSG-n . ., 25.Mai 20 . .)**

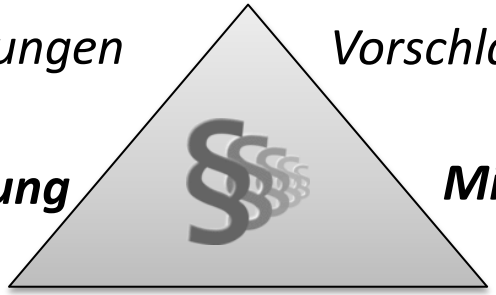
Rechtsakte mit allgemeiner Geltung (Verordnungen und Richtlinien)

Europäischer Rat
Strategische Vorgaben

Europäischer Kommission
Entwirft neue Rechtsvorschriften anhand der Vorgaben des Rates

Trilog-Verhandlungen

Vorschläge der Kommission



Mitbestimmung

Mitbestimmung

Europäisches Parlament

Rat der EU (Ministerrat)

Neue Rechtsvorschriften müssen sowohl vom Europäischen Parlament wie auch vom Rat der EU angenommen werden.

Triloge sind informelle Verhandlungen zwischen dem Europäischen Parlament, dem Rat und der Kommission mit dem Ziel, frühes Einvernehmen zu EU-Gesetzen zu erreichen.

Die Zeittafel der EU-DS-GVO

Auf nationaler deutscher Ebene müssen die vorhandenen gesetzlichen Regelungen (vor allem das BDSG Novelle III von 2009) noch an die **DS-GVO** angepasst werden (Öffnungsklauseln“).

24. Mai 2016
Die DS-GVO ist in Kraft. Damit kann der nat. Gesetzgeber die Vorgaben der DS-GVO zum Erlass ergänzender nationaler Regelungen – Öffnungsklauseln (etwa für ein „neues BDSG IV“) nutzen.

4. Quart. 2016
Bis Herbst 2016 sind die neuen Gesetzentwürfe für die ergänzenden nationalen Regelungen zu erwarten. Derzeit befinden sich diese in der Ausarbeitungsphase.

1. Quart. 2017
Der Bundestag und Bundesrat berät die Gesetzentwürfe für die nationalen Regelungen, zu erwarten im Frühjahr 2017.

4. Quart. 2017
Ablauf der Legislaturperiode und automatischer Verfall von noch nicht verabschiedeten Gesetzentwürfen (z.B. für ein sog. „neues BDSG IV“ - Diskontinuitätsprinzip). Neuer Bundestag und Bundesrat kann neue Gesetzesinitiative zur Verabschiedung starten.

24. Mai 2018
Bis 24. Mai 2018 - Anwendbarkeit des geltenden BDSG (entweder BDSG Novelle III oder „neues BDSG IV“, noch keine Anwendbarkeit der DS-GVO für juristische Personen, Behörden oder für Betroffene.

25. Mai 2018
Anwendbarkeit der DS-GVO und Anwendbarkeit des „neuen BDSG IV“ (insofern verabschiedet). Die BDSG Novelle III von 2009, ist nicht mehr anwendbar.

Die Datenschutz-Grundverordnung (DS-GVO) - Auszug

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur **Aufhebung der Richtlinie 95/46/EG** (Datenschutz-Grundverordnung) – Angenommen vom Rat am **8. April 2016**.

ZIELSETZUNG Erwägungsgrund 11 der Datenschutz-Grundverordnung (DS-GVO)

Haben wir ein Grundrecht auf Privatheit?

ErwGr. 11 - Ein unionsweiter wirksamer Schutz pbD erfordert die Stärkung und präzise Festlegung der Rechte der betroffenen Personen sowie eine Verschärfung der Verpflichtungen für diejenigen, die pbD verarbeiten und darüber entscheiden, ebenso wie - in den Mitgliedstaaten - gleiche Befugnisse bei der Überwachung und **Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie gleiche Sanktionen im Falle ihrer Verletzung.**

Ja, dies haben wir sehr wohl! EU-Grundrechtecharta Art. 1 i.V.m. Art. 1 Abs. 1 GG „Die Würde des Menschen ist unantastbar" Art. 7 „Achtung des Privat- und Familienlebens...". Die DS-GVO „Diese VO schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz pbD" – BDSG(neu)...

Wesentliche Umsetzungsmaßnamen bez. der Vorbereitung auf die DS-GVO

Übersicht der Handlungsempfehlungen zur Umsetzung der DS-GVO bis zum Stichtag: 25. Mai 2018

Die Projektinitialisierung erfolgt durch die Geschäftsleitung - Verantwortlicher

Phase I mit sehr hoher Dringlichkeit

- **Bestellung** des Datenschutzkoordinators
- **Unterweisung** des Datenschutzkoordinators
- **Erstellung** des Verzeichnisses von Verarbeitungstätigkeiten
- **Sensibilisierung** der Mitarbeiter, Datenschutz-Unterweisung
- **Beurteilung** der Datenschutz-folgeabschätzung

Phase II mit hoher Dringlichkeit

- **Implementierung der Auskunftserteilung**, und die Übertragung personenbezogener Daten
- **Überprüfung und Anpassung** von Vertragsvorlagen und Einwilligungserklärungen
- **Überarbeitung der Dokumentationen** mit Auftragsdaten-verarbeitern
- **Aktualisierung und Überarbeitung** des Datenschutz-Handbuchs
- **Neuaufstellung** des betriebl. bzw. externen Datenschutzbeauftragten

Phase III mit mittlerer Dringlichkeit

- **Implementierung der Prozesse** "Privacy by Design" und by Default"
- **Festlegung und Überarbeitung** der TOM inkl. risikobasiertem Ansatz
- **Überprüfung der** Verschlüsselungs-, Anony-misierungs & Pseudony-misierungs Möglichkeiten
- **Einführung eines kontinuierlichen** Verbesserungsprozesses – PDCA –ISO 27001
- **Identifikation und Kontaktaufnahme** mit der Zuständigen Aufsichtsbehörde

Die Systematik (Aufbau) - Der DS-GVO I (Table of Contents)

Art. 9 DS-GVO Verarbeitung besonderer Kategorien pbD I

Processing of special categories of personal data

Artikel 9 Verarbeitung besonderer Kategorien personenbezogener Daten

Abs. 1 Die Verarbeitung pbD, aus denen die

1. **rassische und ethnische Herkunft**,
2. **politische Meinungen**,
3. **religiöse oder weltanschauliche Überzeugungen** oder die
4. **Gewerkschaftszugehörigkeit** hervorgehen, sowie die Verarbeitung von
5. **genetischen Daten**,
6. **biometrischen Daten** zur eindeutigen Identifizierung einer natürlichen Person,
7. **Gesundheitsdaten** oder Daten zum
8. **Sexualleben** oder der **sexuellen Orientierung** einer natürlichen Person

ist untersagt.

Die Erhebung dieser Daten ohne Rechtsgrundlage löst eine Meldepflicht (Datenschutzpanne) **gemäß Art. 33 DS-GVO aus.**

Es können *Bußgelder bis zu 20 Mio. €* gemäß Art. 83 Abs. 5 DS-GVO verhängt werden!

Wen oder was schützt die DS-GVO?

Kreuzen Sie bitte die richtigen Lösung an.

Datenschutzkonforme Datenverarbeitung I

Bei den Prozessen der datenschutzkonformen Datenverarbeitung stellt sich die Frage, welche Anforderungen ein Unternehmen erfüllen muss, **damit die Verarbeitung personenbezogener Daten im Einklang mit der DS-GVO erfolgt**.

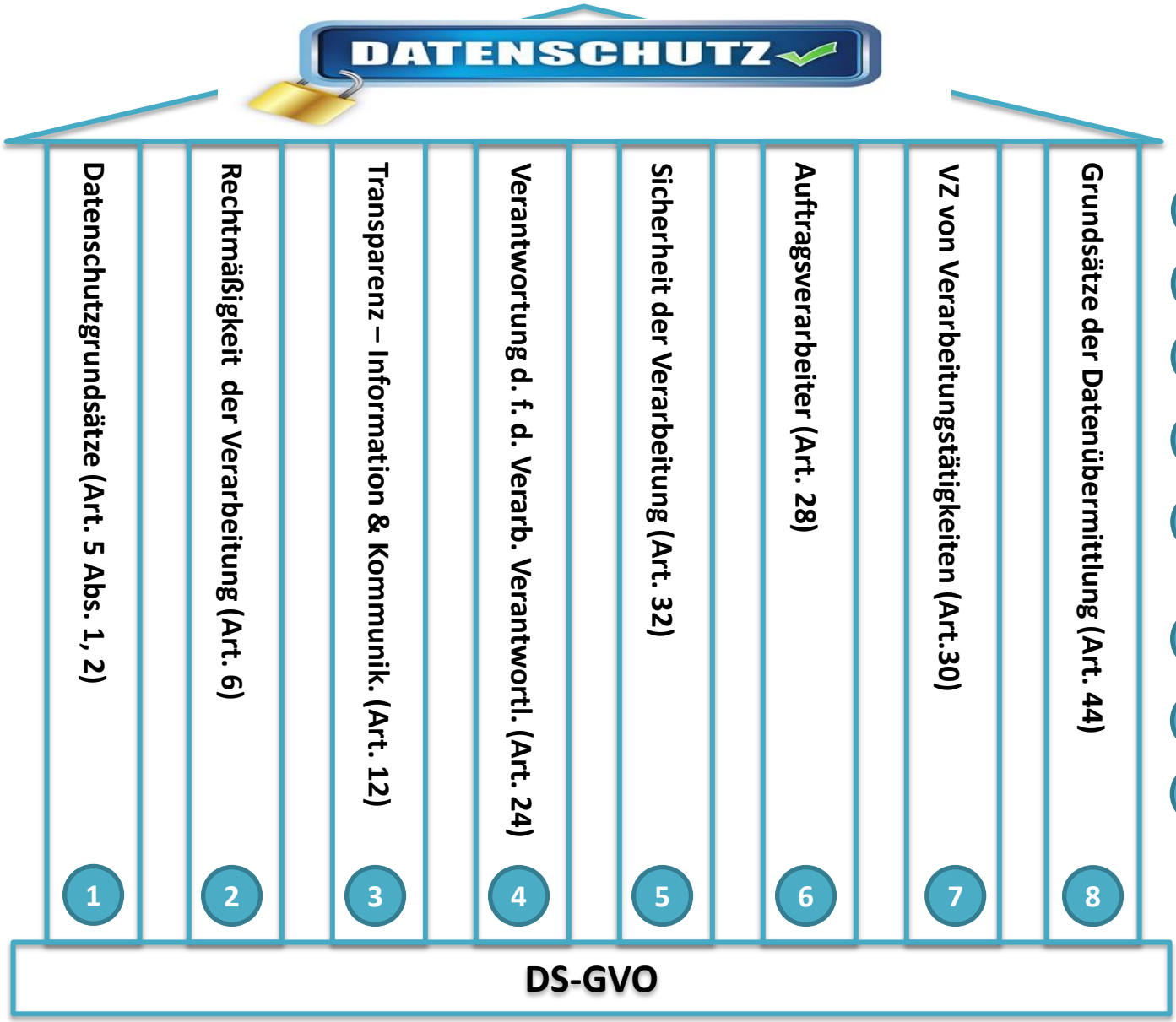
Überblick Datenverarbeitung:
Die rechtmäßige Datenverarbeitung ist an folgende Voraussetzungen geknüpft:

- Der Einhaltung der Datenschutzgrundsätze (**Art. 5 Abs. 1, 2**)
- Die Rechtmäßigkeit der Verarbeitung basierend auf den Rechtsgrundlagen (**Art. 6**)
- Transparenz zur Erhebung durch angemessene Information der betroffenen Person (**Art. 12**)
- Die Sicherheit der Verarbeitung durch Umsetzung geeigneter TOM‘s (**Art. 24, 32**)
- Die Datenschutzkonforme Auftragsverarbeitung, u.a. durch geeignete TOM‘s (**Art. 28**)
- Die Dokumentation der Verarbeitungstätigkeiten **(Art. 30**)
- Die Sicherstellung des Schutzniveaus bei der Übermittlung pbD in Drittländer (**Art. 44**)

Allgemeine gesetzliche Erlaubnistatbestände für die Verarbeitung pbD ergeben sich aus Art. 6 Abs. 1 lit. a-f.
Hiernach dürfen personenbezogene Daten zu folgenden Zwecken verarbeitet werden:

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung gegeben (**Art. 6 Abs. 1 lit. a**),
- zur Erfüllung vertraglicher- und vorvertraglicher Pflichten (**Art. 6 Abs. 1 lit. b**),
- zur Erfüllung rechtlicher Pflichten (**Art. 6 Abs. 1 lit. c**) z.B. Finanzbuchhaltung (§ 238 Abs. 1 HGB),
- zum Schutz lebenswichtiger Interessen (**Art. 6 Abs. 1 lit. d**),
- zur Wahrnehmung öffentlicher Interessen und zur Ausübung öffentlicher Gewalt (**Art. 6 Abs. 1 lit. e**)
- sowie zur Wahrung berechtigter Interessen (**Art. 6 Abs. 1 lit. f**) z.B. Marketing, Forschungsfreiheit.

Datenschutzkonforme Datenverarbeitung nach DS-GVO



1. **Rechenschaftspflicht gemäß Art. 5 Abs. 2**
2. **Rechtsgrundlage & Zweck**
3. **Informations- und Kommunikationspflicht**
4. **Geeignete TOM vorh.?**
5. **TOM vorh.? & Gewährl.** der Vertraulichkeit, Integrität, Verfügbarkeit…
6. **Geeignete TOM vorh.? & Auswahl & AV-Vertag**
7. **Dokumentationspflicht**
8. **„Drittland“, Schutz-niveau gewährleistet? &** Binding Corporate Rules

Die drei Kernprozesse im Datenschutz gemäß DS-GVO

General Data Protection Regulation

1 Rechtsverbindliche Datenverarbeitung von personenbezogenen Daten

Jede Verarbeitung von pbD bedarf einer Rechtsgrundlage.

- **Datenschutzgrundsätze** Art. 5 Abs. 1, 2
- **Rechtmäßigkeit der Verarbeitung** Art. 6
- **Auftragsverarbeiter** Art. 28
- **VZ von Verarbeitungstätigkeiten** Art.30
- **Grundsätze der Datenübermittlung** Art. 44

Die Überprüfung der TOM sind bspw. ein weiter Prozess.

2 Sicherstellung und Gewährleistung der Betroffenenrechte

Die Betroffenenrechte sind zu gewährleisten - (informationelle Selbstbestimmung).

Die **transparenten Mitteilungspflichten** an die **Betroffenen** stellen einen weiteren wichtigen Kernprozess für das Unternehmen dar (z.B. durch das Auskunftsrecht).

Die Betroffenenrechte sind ein wesentlicher Bestandteil der DS-GVO und in den Unternehmensalltag ebenfalls zu integrieren.

3 Die Handhabung von Datenschutzverletzungen und die rechtzeitige Erkennung

Einen weiteren Geschäftsprozess stellt die Handhabung von Datenschutzverletzungen **gemäß Art. 4 Nr. 12**, dar.

Welche eine Melde- und Benachrichtigungspflicht auslösen können (z.B. durch das Abhandenkommen von pbD **gemäß Art. 9 DS-GVO**).

Eine Verletzung des Schutzes pbD liegt vor, wenn ein Verlust, eine Veränderung / eine unbefugte Offenlegung oder ein unbefugter Zugang zu pbD stattgefunden hat.

Geschäftsprozesse nach Fachabteilungen (Geschäftsprozess-Matrix)

	Geschäftsprozess-Nr.																									
Fachabteilungen	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
F0 (GL)	X	X			X	X																				X
F0.1 (AM)	X	X				X																				
F0.2 (BR)	X					X																				
F0.3 (BH)	X					X																				
F0.4 (Contrl)	X					X																				
F0.5 (DS)	X					X																				
F0.6 (Eink)	X					X																				
F0.7 (Empfang)	X			X		X																				
F0.8																										
F0.9	X	X				X																				
F0.10						X																				
F0.11	X																									
F0.12																										
F0.13						X																				
F0.14	X					X																				
F0.15																										
F0.16	X					X																				
F0.17	X					X																				
F0.18	X					X																				
F0.19		X				X																				
F0.20	X					X																				
F0.21	X					X																				
F0.22	X				X	X																				X

Fachabteilungen und die Prozessverantwortlichen (Abteilungsleiter)

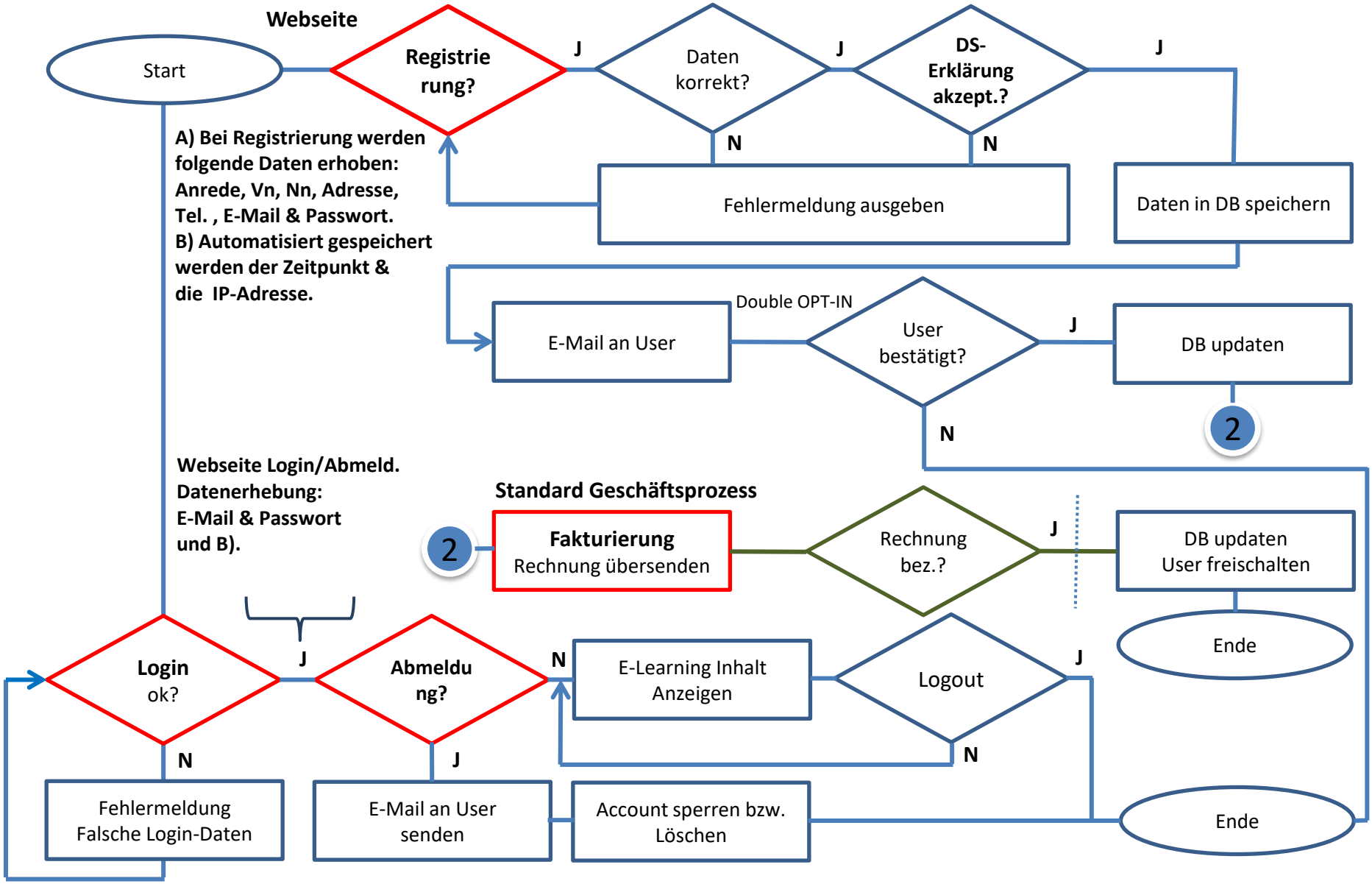
F-Nr.:	Bezeichnung	Abtl. / Prozessv.	F-Nr.:	Bezeichnung	Abtl. / Prozessv.
F0.0	Geschäftsleitung	Herr A. Müller	F0.13	Konstruktion	Frau E. Groß
F0.1	Auftragsmanagement	Frau B. Maier	F0.14	Kundenmanagement	Herr F. Müller
F0.2	Betriebsrat	Herr C. Schmitt	F0.15	Lager	x
F0.3	Buchhaltung	Frau D . Duck	F0.16	Logistik	x
F0.4	Controlling	x	F0.17	Marketing	x
F0.5	Datenschutz	x	F0.18	Personal	x
F0.6	Einkauf	x	F0.19	Revision	x
F0.7	Empfang / Rezeption	x	F0.20	Service / Callcenter	x
F0.8	Fertigungsplanung	x	F0.21	Vertrieb	x
F0.9	Finanzen	x	F0.22	DS-GVO	Frau G. Mayer
F0.10	Fuhrpark	x		Gewährleistung	der betroffenen
F0.11	IT	x		Rechte gemäß	Art. 12 bis 23 und
F0.12	Kantine	x		Art. 28, Art. 30, Art. 33	DS-GVO etc.

Beispiel für Verfahren („Verarbeitungstätigkeiten")

GP-Nr.:[1]	Bezeichnung	GP-Nr.:[1]	Bezeichnung
1	Adressen und Kontaktdaten (Excel)	15	Mobile-/Handy-/Smartphone-Nutzung
2	Bestellwesen, Fakturierung, Zahlungseing.	16	Notfallkonzept
3	Barkasse	17	PC Login
4	Besuchermanagement	18	Projektmanagement
5	Betroffenen Rechte Art. 12 bis 23 DS-GVO	19	Prüfung gegen Antiterrorlisten
6	Bürokommunikation	20	Reisemanagement
7	Daten an StB/WP/Zollbehörden	21	Schutz- und Arbeitskleidung
8	Daten an Unternehmensberater	22	Verbesserungsprozess
9	Dokumentenmanagementsystem	23	Vertragsverwaltung
10	Druck- und Kopieraufträge	24	Videoüberwachungsanlage
11	E-Learning	25	Zutritt Fremdarbeiter
12	Groupwaresystem	26	Auftragsverarbeiter Art. 28 DS-GVO
13	Gäste-WLAN		
14	Kundenverwaltung		

Abb. Fachabt. & Verfahren

Vereinfachte systematische Darstellung der Prozessabläufe – E-Learning



Die neuen Sanktionen bzw. Bußgelder der DS-GVO

Artikel 83 Abs. 4	Artikel 83 Abs. 5	Artikel 83 Abs. 6
bis 10 Mio. € oder bis 2% des weltweiten Vorjahres-umsatzes	**bis 20 Mio. € oder bis 4% des weltweiten Vorjahresumsatzes**	**bis 20 Mio. € oder bis 4% des weltweiten Vorjahresumsatzes**
Verstöße gegen Regelungen z.B. im Bereich: • Schutzmaßnahmen (TOM) • Auftragsverarbeitung bzw. Auftragsverarbeiter • Verzeichnis der Verarbeitungstätigkeiten • Datenschutz Folgenabschätzung • Bestellung des Datenschutz-beauftragten…	Verstöße gegen Regelungen z.B. im Bereich: • Grundsätze (Art. 5) • Treu und Glaube • Rechtmäßigkeit z.B. Verarbeitung besonderer Kategorien pbD (Art. 9) • Einwilligung • Rechte Betroffener • Drittlandsübermittlung • Zusammenarbeit mit Aufsichtsbehörde…	Verstöße gegen Anordnungen der Aufsichtsbehörde. Die Bußgeldtatbestände der DS-GVO sind in Art. 83 Abs. 4, 5, 6 geregelt.  

Bei Verstößen gegen Tatbestände der zweiten Gruppe gemäß Art. 83 Abs. 5 und 6 DS-GVO sind in jedem Einzelfall Bußgelder zu verhängen, die wirksam, verhältnismäßig und abschreckend sind.

Urheberrechte - Bildernachweis

Alle Bilder welche zur optischen Unterstützung des Lernenden im Seminar: „Betrieblicher Datenschutzbeauftragter“ gemäß DS-GVO & BDSG dienen, wurden erworben bei:

https://de.depositphotos.com oder bei http://de.fotolia.com

Quellangaben:
BDSG III von 2009, BDSG(neu), EU-DSG-VO (http://eur-lex.europa.eu/homepage.html), www.bfdi.bund.de, www.bsi.bund.de, https://www.datenschutz-bayern.de, ww.lfd.niedersachsen.de, https://www.datenschutzzentrum.de, Datenschutz-Compliance nach der DS-GVO – Autoren: Kranig · Sachs · Gierschmann

Danke für Ihre Aufmerksamkeit

Allgemeiner Hinweis:
Wer Zeigefinger und Daumen in Deutschland zu einem Kreis formt, möchte damit anzeigen, **dass er etwas gut findet** oder das Essen ausgezeichnet schmeckt. Auch in der Tauchersprache bedeutet dieses Zeichen, dass alles in bester Ordnung ist. (https://www.welt.de/reise/...)