



***Auswirkungen der DSGVO, des BDSG-  
Neu und der ePrivacy-Verordnung auf ein  
mittelständisches Industrieunternehmen***

**SEW  
EURODRIVE**

ICS Stuttgart **mbuf**  
16.&17. April 2018

**mbufJK18**  
Kongress für Microsoft Business User

A decorative graphic consisting of a cluster of small, colorful diamond shapes in shades of green, yellow, and red, arranged in a roughly circular pattern.

IT-Compliance & Information Security / ITC  
*Datenschutzbeauftragter*

SEW-EURODRIVE GmbH & Co KG  
Ernst-Blickle-Str. 42  
D-76646 Bruchsal

Tel. +49 7251 75-1606  
Fax +49 7251 75-501606  
Mobil +49 172 7261301  
bernhard.haungs@sew-eurodrive.de  
<http://www.sew-eurodrive.de>



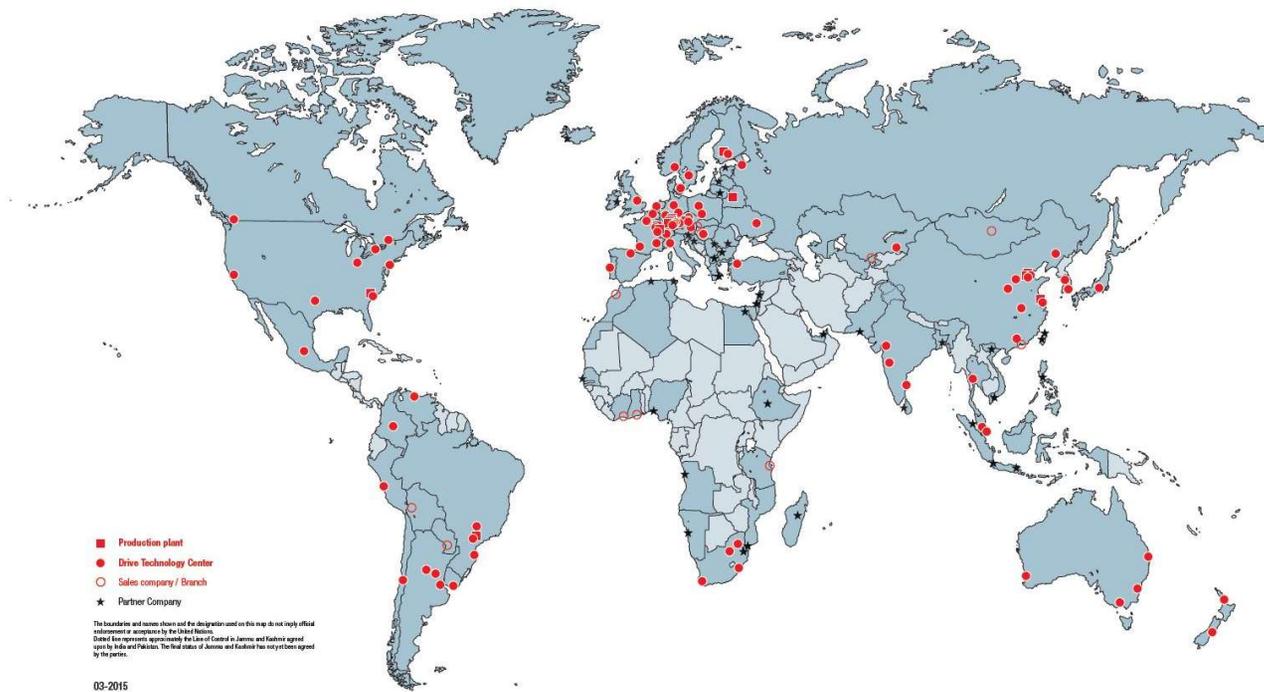
## **Bernhard Haungs**

seit 1998 bei SEW

Rechenzentrum, RZ-Steuerung, Netzwerk,  
PC's, Notebooks, mobile und  
Festnetztelefonie Bürotechnik, SAP-Basis,  
Server, ServiceDesk ....

seit 2004 verantw. für Information Security  
seit 2012 Datenschutzbeauftragter

## International denken, national handeln



Über 16.000  
Mitarbeiter

15 Fertigungswerke  
77 Drive Technology Center

Standorte in  
51 Ländern

2,8 Mrd. €  
Umsatz GJ 2016/2017

Seit  
85 Jahren

Unternehmen **Produkte und Lösungen** Branchen

## Komplettprogramm

Die Antriebstechnik von SEW-EURODRIVE steht für Produktvielfalt, Qualität, Zuverlässigkeit und Innovationskraft.

- Getriebemotoren und Frequenzumrichter
- Servo-Antriebssysteme
- Dezentrale Antriebssysteme
- Industriegetriebe
- Antriebsautomatisierungslösungen
- Systemkomponenten und Dienstleistungen



Unternehmen   Produkte und Lösungen   **Branchen**

## Unsere Branchenkompetenz

Ohne die Antriebstechnik von SEW-EURODRIVE würde auf der Welt vieles stillstehen. Mit Produktvielfalt und Kundennähe begegnen wir den Anforderungen der unterschiedlichsten Branchen und schaffen neue Standards im Markt.

- Transport und Logistik
- Automobilindustrie
- Nahrungsmittel- und Getränkeindustrie
- Bau- und Baustoffindustrie
- Chemie- und Pharmaindustrie
- Holzindustrie, u.v.a.m.



# Auswirkungen von

**DSGVO** → **Europäische Datenschutzgrundverordnung**  
**GDPR** → **General Data Protection Regulation**

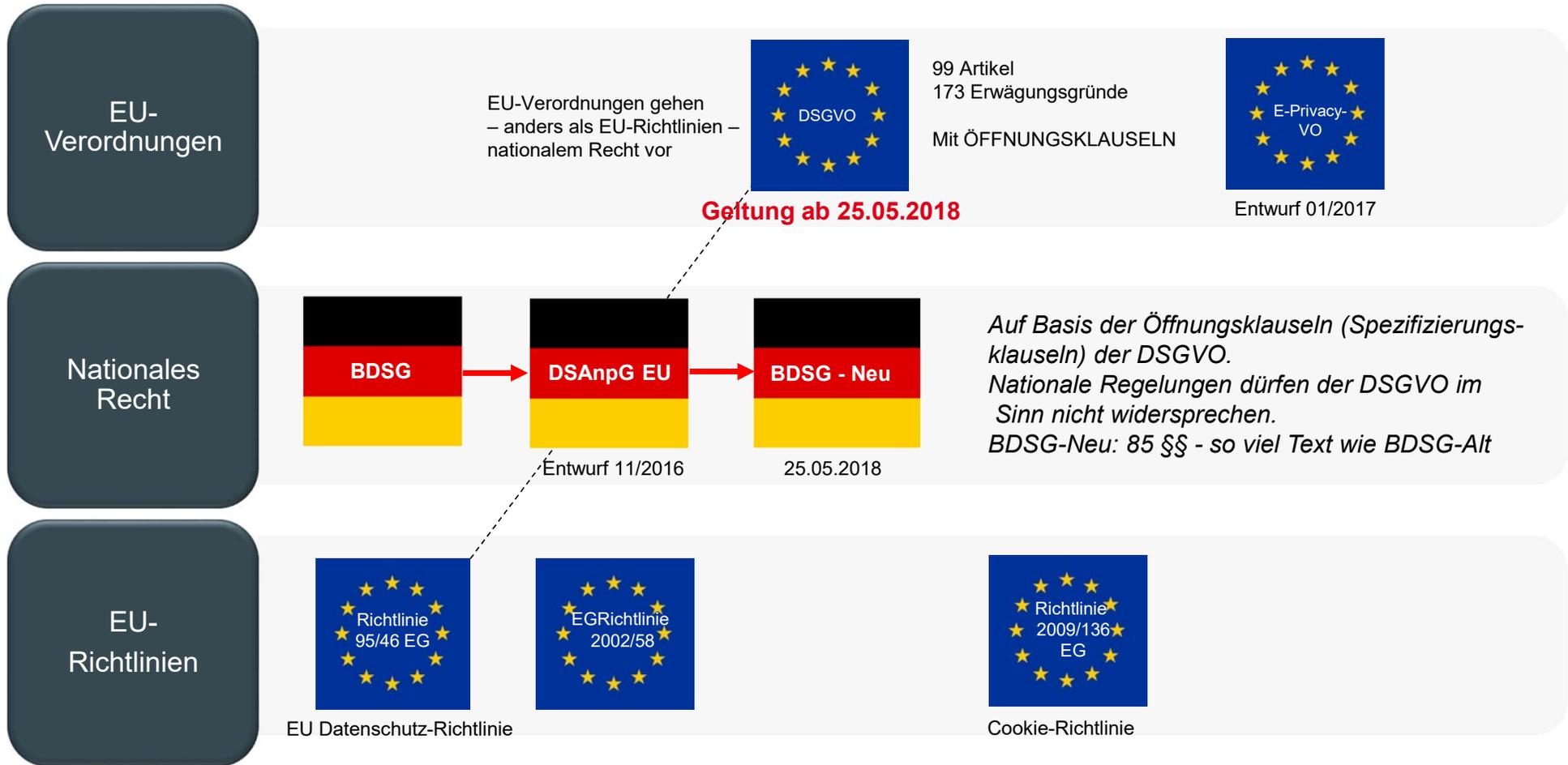
**BDSG-Neu** → **Bundesdatenschutzgesetz – Neu**

**e-Privacy-VO** → **Verordnung über Privatsphäre und elektronische Kommunikation;  
Datenschutz im Internet (frühere „Cookie-Richtlinie“)**

## auf SEW-EURODRIVE GmbH & Co KG

# Gliederung

- Darstellung der relevanten Gesetze/Verordnung
- Warum Datenschutz bei SEW wichtig ist
- Wesentliche Änderungen durch die DSGVO
- Rechtsfolgen bei Verstößen
- Maßgebliche Punkte durch das BDSG-Neu
- Entwurf der ePrivacy-Verordnung
- Vorgehensweise zur Gewährleistung der Compliance
- Darstellung der Maßnahmen



## Warum Datenschutz bei SEW wichtig ist

- „Compliant“ zu Rechtsvorschriften aus HGB, AO, GoBD, KonTraG, BetrVG ..... und dem Datenschutzgesetz
- Schutz der Persönlichkeitsrechte der SEW-Mitarbeiter -> Arbeitnehmer, Leiharbeitnehmer, Studenten, Auszubildende, Bewerber.  
„Jede Verarbeitung personenbezogener Daten benötigt einen erlaubten Zweck“

- Schutz der Persönlichkeitsrechte von Ansprechpartner bei Kunden und bei Lieferanten

SEW = Business to Business Company (nicht B to Consumer)

Keine personenbezogenen Daten aus dem Privatbereich von Kunden, Lieferanten und Geschäftspartner

- **Verlässlicher Datenschutz ist Teil der Werte des sozialen Miteinanders.**



# Kernpunkte der Datenschutzgrundverordnung DSGVO aus 99 Artikel und 173 Erwägungsgründen



Die EU-DSGVO (EU-Verordnung 2016/679), die am 25. Mai 2018 in Kraft tritt, gibt den Einzelpersonen die Kontrolle und den Schutz ihrer personen-bezogenen Daten.

## **Wer muss diese Verordnung befolgen?**

Organisationen, die EU-Bürgern Waren oder Dienstleistungen anbieten oder deren Verhalten überwachen oder personenbezogene Daten von EU-Bürgern verarbeiten (erheben, speichern, in Zusammenhänge setzen, weitergeben, löschen)

## **Auf wen wird die EU-DSGVO angewandt (Betroffene)?**

Natürliche Personen, unabhängig von deren Nationalität oder Wohnort, betreffend die Verarbeitung derer personenbezogener Daten.

## Wesentliche Änderungen durch die DSGVO (1/3)

### ➤ **Marktortprinzip**

Danach gilt das europäische Datenschutzrecht künftig auch für außereuropäische Unternehmen, wenn diese Waren oder Dienstleistungen im europäischen Markt anbieten.

### ➤ **Betroffenenrechte**

werden deutlich ausgeweitet und es wird eine Reaktionszeit verbindlich festgelegt.

Der Prozess der Wahrung der Betroffenenrechte muss in der Dokumentation definiert sein. Neu ist:

#### ▪ **Recht auf Vergessenwerden**

Betroffenen steht bei der Durchsetzung ihres Löschungsanspruchs gegenüber Dritten von der verantwortlichen Stelle stärkere Unterstützung zu als bisher.

#### ▪ **Recht auf Datenübertragbarkeit**

Die Nutzer sozialer Netzwerke können vom jeweiligen Anbieter des Netzwerks die Herausgabe ihrer Daten in einem Format verlangen, das es ihnen ermöglicht, diese Daten bei einem anderen Anbieter weiter zu nutzen.

## Wesentliche Änderungen durch die DSGVO (2/3)

- **Konzernprivileg**  
Der für Unternehmen interessanteste neue Begriff, der in Artikel 4 definiert wird, ist die sog. **Unternehmensgruppe**. Darunter versteht man eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht. Mit Codes of Conduct
- **Privacy by Design/Privacy by Default**  
Die Datenschutzrechte der Betroffenen werden im Vorfeld gestärkt, indem bereits Hersteller und Verantwortliche zu datenschutz-freundlichen Produkten und Voreinstellungen – und auch in Prozessen – verpflichtet werden.
- **Rechenschaftspflicht**  
Der Verantwortliche muss die Einhaltung der Artikel der DSGVO nachweisen können.
- **Dokumentationspflichten**  
werden deutlich ausgeweitet. Das Datenschutzmanagement muss jederzeit nachgewiesen werden

## Wesentliche Änderungen durch die DSGVO (3/3)

### ➤ **Datenschutz-Folgenabschätzungen**

Für Datenverarbeitungen mit bestimmten Risiken ist künftig die Durchführung einer Datenschutz-Folgenabschätzung verbindlich vorgeschrieben. Diese muss von der Stelle durchgeführt werden, die für die Verarbeitung verantwortlich ist.

### ➤ **Selbstregulierung und Zertifizierung**

Die DS-GVO sieht einen Rahmen für die Schaffung von Verhaltensregeln und Zertifizierungsverfahren vor.

### ➤ **Beibehaltung der Zweckbindung im bisher gültigen Umfang – Erlaubnistatbestände**

Der Grundsatz der Zweckbindung gilt weiterhin als eine tragende Säule des Datenschutzrechts.

- **Gesetzliche Pflichten oder Vertragserfüllung**
- **Einwilligung oder Betriebsvereinbarung**
- **Interessenabwägung – *betriebliches Interesse und keine Anhaltspunkte, dass schutzwürdige Interessen von Betroffenen verletzt werden.***

## Rechtsfolgen bei Verstößen

- **Haftung für Ordnungswidrigkeiten**  
Bußgelder bis zu 20 Millionen Euro oder bis zu 4% des weltweit erzielten Jahresumsatzes (Artikel 83 Abs. 4,5) je nachdem, welcher Wert der Höhere ist.  
→ *gilt nicht für Einrichtungen des öffentlichen Dienstes*
- **Haftung auf Schadensersatz**  
Materielle und immaterielle Schäden; Beweislastumkehr
- **Verantwortlicher**  
ist die natürliche oder juristische Person, Behörde, Einrichtung oder anderer Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DSGVO)
- **Ggf persönliche Haftung der Geschäftsleitung**  
GmbH Gesetz § 43, Absatz 1 und 2



# Aufsichtsbehörden

- **Art 60 – 62** regeln die Zusammenarbeit, die Amtshilfen und die Kohärenz (im Sinne der einheitlichen Anwendung der Verordnung) der Aufsichtsbehörden untereinander

- **Aufsichtsbehörde Baden-Württemberg:**

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Dr. Stefan Brink

- Beratung – nach Anfrage
- Kontrolle
- Verfolgt Hinweise/Beschwerden; auch anonyme. Erwartet von Privatpersonen, Wettbewerber und Beschäftigte.  
Und: Verbraucherzentralen und Datenschutzvereine (Art 80). Abmahnungswesen als Betätigungsfeld
- Verhängt Bußgelder (wirksam, verhältnismäßig, abschreckend (IHK KA am 24.10.2017))
- Ca. 50 Mitarbeiter
- Nicht zuständig für kirchliche Einrichtungen und nicht für Rundfunkanstalten
- 5 zusätzliche Stellen für Bußgeldreferat beantragt



## Maßgebliche Punkte durch BDSG-Neu für SEW

### ➤ **Verarbeitung besonderer Kategorien von Daten ( § 22 )**

**Art 9 DSGVO:** Die Verarbeitung personenbezogener Daten, aus denen die **rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit** hervorgehen, sowie die Verarbeitung von **genetischen Daten, biometrischen Daten** zur eindeutigen Identifizierung einer natürlichen Person, **Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung** einer natürlichen Person **ist untersagt** .

**§ 22 BDSG-Neu:** erlaubt zum Zweck der Gesundheitsvorsorge, aus Gründen öffentlichen Interesses, Gemeinwohls, Verteidigung .....

### ➤ **Verarbeitung im Beschäftigungskontext ( § 26 )**

Sehr ähnlich des bisherigen § 32 BDSG. Verarbeitung von Beschäftigtendaten zulässig bei positiver Interessenabwägung. Betriebsvereinbarungen weiterhin rechtswirksam.

Gültig auch für Leiharbeiter, Auszubildende, Studenten, Bewerber und Rentner.

Im Erwägungsgrund 48 zur DSGVO wird die Übermittlung von Beschäftigtendaten „innerhalb der Unternehmensgruppe für interne Verwaltungszwecke“ ausdrücklich als mögliches berechtigtes Interesse des Unternehmens aufgeführt.

## **e-Privacy-VO → Verordnung über Privatsphäre und elektronische Kommunikation; Datenschutz im Internet („Cookie-Richtlinie“)**

- Anpassung der EU-Vorgaben aus der E-Privacy-Richtlinie („Cookie-Richtlinie“) an die DSGVO und neue Entwicklungen
- Aktuelle Fassung: Entwurf der EU-Kommission von Januar 2017
- Zeitplan offen. Ursprünglich geplanter Termin: 25. Mai 2018 – Übergangsfrist erwartet
- Erstreckung auf Over-the-Top-Dienste (OTT) wie WhatsApp usw. Bei der Nutzung von Kommunikationsdiensten wie WhatsApp, Facebook-Messenger, Facetime oder klassischer Telefonie fallen **viele Daten über das Verhalten der Nutzer** an. Die Kommunikationsdienstleister wollen diese Informationen analysieren und verwerten, beispielsweise für die Personalisierung von Werbung. **Im Entwurf: Nur mit Einverständnis des Betroffenen!** Außerdem sollen sogenannte **Tracking-Walls** verboten werden, bei denen Websitebetreiber den Zutritt zu ihrer Webseite davon abhängig machen, dass man einer Aufzeichnung des eigenen Verhaltens zustimmt.
- **Recht auf Verschlüsselung.** Den **EU-Mitgliedsstaaten** soll es zudem **nicht gestattet** sein, Gesetze zu erlassen, mit denen sie Anbieter von Kommunikationsdiensten oder -software zwingen, die Vertraulichkeit und Integrität der Kommunikation ihrer Nutzer zu schwächen

## e-Privacy-VO (2)

- Cookie-Nutzung (Art. 8):
  - Ist grundsätzlich untersagt. Außer:
  - Ist für den alleinigen Zweck der Durchführung des elektronischen Kommunikationsvorgangs nötig, oder
  - Einwilligung liegt vor.
  - Auch hier Kopplungsverbot
- Datenverarbeitung zu E-Mail-Werbung (Art. 16):
  - Grundsatz: Elektronische Kommunikation für Direktmarketing **nur nach Einwilligung** (Abs. 1)
  - Werbung möglich bei Datenerhebung im Rahmen eines Vertragsabschlusses, bei Informationen über einfachen und kostenlosen Widerspruch (Abs. 2)
  - Fazit: Praktisch keine Änderung zu § 7 UWG
- Telefonwerbung (Art. 16):
  - Verschärfung geplant
  - Telefonwerbung selbst im B2B-Geschäft **nur nach Einwilligung** eines Ansprechpartners (Abs. 1)
  - Zusätzliche Anforderungen, wie Identifikation (Abs. 3)
  - Öffnungsklausel für Mitgliedsstaaten (Abs. 4)

## Vorgehensweise zur Gewährleistung der Compliance bei SEW

- 5. September 2017**    **1. Tagesworkshop mit Vertretern aus Vertrieb, Marketing, Personalwesen und IT**
- Präsentation der Rechtsgrundlagen durch RA Dr. Matthias Lachenmann von Pauly & Partner, Bonn
  - Erhebung der SEW-Verfahren mit personenbezogenen Daten
- 16. Oktober 2017**    **2. Tagesworkshop mit gleichem Teilnehmerkreis**
- Evaluierung von generellen organisatorischen und technischen Maßnahmen
  - Darstellung der Bewertung der SEW-Verfahren vom 1. Workshop
- November 2017**    **Erstellung von Maßnahmenplan, Verantwortlichkeiten, Terminplan und Budget**
- 28. November 2017**    **Präsentation bei GF; Verabschiedung und Mittelfreigabe**
- Dez 2017 – Mai 2018**    **Umsetzung des Maßnahmenplanes**

Geschätzter Aufwand: ca 260 PT

davon 81 BDSB,

40 Legal,

91 IT,

Rest Personal, IP, CC, VB2



## Maßnahmen zur Gewährleistung der Compliance (1a)

Erweiterung/ Aufbau Verzeichnis von Verarbeitungstätigkeiten (Verfahrensbeschreibung)

Aufwand: 40 PT, Rechtsgrundlage: Art 30

Laufende Nummer	Verfahrensbezeichnung	Kurzbeschreibung des Verfahrens	IT-Zuständigkeit	Regionale Verfügbarkeit	Arten der personenbezogenen Daten	Betroffene Personengruppen	Datenherkunft	Zugriffsberechtigte	Rechtsgrundlage der Verarbeitung	Auftragsdatenverarbeitung	Datenübermittlung in Drittstaaten	Aufbewahrung sfristen
5	Globaler IT-Service-Desk	Abwicklung aller Anfragen und Störungsmeldungen in der Nutzung der IT-Dienstleistungen	ITSD	SEW Deutschland und andere Landesorganisationen	Name, eMail-Adresse, Personalnummer, Windows-Anmeldename, Organisationseinheit, Gebäude/Raum, Kostenstelle, Beschäftigungsstatus,	Mitarbeiter, Leiharbeiter	SAP-HCM	jeder "helpLine"-User in Deutschland	§ 28 BDSG	nein	nein	10 Jahre

Verfahrensverzeichnis alt: < 20 Einträge

Verzeichnis der Verarbeitungstätigkeiten mit personenbezogenen Daten: > 150 Einträge (geschätzt)

Zusätzliche Angaben notwendig:

Namen und Kontaktdaten des Verantwortlichen und des bDSB  
**Zweck der Verarbeitung, Löschkonzept**

## Maßnahmen zur Gewährleistung der Compliance (1b)

Erweiterung/ Aufbau Verzeichnis von Verarbeitungstätigkeiten (Verfahrensbeschreibung)

Aufwand: 40 PT, Rechtsgrundlage: Art 30

Laufende Nummer	Verfahrensbezeichnung	Kurzbeschreibung des Verfahrens	IT-Zuständigkeit	Regionale Verfügbarkeit	Arten der personenbezogenen Daten	Betroffene Personengruppen	Datenherkunft	Zugriffsberechtigte	Rechtsgrundlage der Verarbeitung	Auftragsdatenverarbeitung	Datenübermittlung in Drittstaaten	Aufbewahrung sfristen
5	Globaler IT-Service-Desk	Abwicklung aller Anfragen und Störungsmeldungen in der Nutzung der IT-Dienstleistungen	ITSD	SEW Deutschland und andere Landesorganisationen	Name, eMail-Adresse, Personalnummer, Windows-Anmeldename, Organisationseinheit, Gebäude/Raum, Kostenstelle, Beschäftigungsstatus,	Mitarbeiter, Leiharbeiter	SAP-HCM	Jeder "helpLine"-User in Deutschland	§ 28 BDSG	nein	nein	10 Jahre

**Stand 8. März 2018:** Formular mit Ausfüllanleitung und Beispielverfahren (Fuhrparkmanagement GFFP)

**19.2. versendet** an EKL, FAL, FCL, PL, SM, SIG, SE, BUM, BUH-S, AM, BUC

Mit VB2-PK, IPS, CC, ISI und IT intensiver Kontakt zu CRM-Kundenstamm, Newsletter, Datenschutzhinweise, Tracking etc

Mit Personalbereich > 40 Verfahren in Abstimmung.

**12.3. versendet** an EDG, GGW, WGF, WGL, PSRM, ISL, WBE, QML, BFM

Anfang April dann die restlichen

## Maßnahmen zur Gewährleistung der Compliance (2)

Datenschutz Prozessbeschreibung (analog ISMS nach ISO27001)

Aufwand: 10 PT, Rechtsgrundlage: Art 5, 24

- Beschreibung Verantwortlichkeiten, Rollen
- Beschreibung Datenschutz Leitlinien
- Verzeichnis der Verfahren
- Prozessbeschreibung Behandlung Betroffenenrechte
- Schulungs- und Sensibilisierungskonzept
- Formular Auftragsdatenverarbeitung
- Kontakt zu Aufsichtsbehörde
- Beschreibung Datenschutzfolgeabschätzung
- Prozessbeschreibung Datenübermittlung im Unternehmensverbund
- Prozessbeschreibung Datenschutz-Sicherheitsvorfälle
- Organisationsanweisung
- Verpflichtungserklärung zum Arbeitsvertrag
- .....
- *Teile davon Publikation im DriveNet*







## Maßnahmen zur Gewährleistung der Compliance (4)

Tracking auf Homepage und Online Services  
Aufwand: 22 PT, Rechtsgrundlage: Art 6, 7

- Information des Users über Tracking
- Schaffung Opt-out-Möglichkeit
- Anonymisierung der IP-Adresse
- Verarbeitung Userbezogene Trackingdaten:  
**Separate Einwilligung zwingend notwendig**
- Zeitliche Begrenzung von Cookies



## Maßnahmen zur Gewährleistung der Compliance (5)

Bereich Personal Beschäftigtendatenschutz

Aufwand: 32 PT, Rechtsgrundlage: Art 5, 24, 40, 88 und §26

Personalwesen



- Beschreibung jedes einzelnen Prozesses im Verzeichnis

Gehaltsabrechnung, Zeiterfassung, Bewerbermanagement, Beurteilungsverfahren, Personalentwicklungsverfahren, Führerscheinkontrolle, Reisekostenabrechnung, Auswertungen uvm nach allen Kriterien gemäß Art 30 DSGVO geschätzt > 40

- Erstellung Organisationsanweisung zeitnah zum 25.5.2018
- Prozessbeschreibung zur Wahrung der Betroffenenrechte (Mitarbeiter, Rentner, Leiharbeiter, Azubis, Studenten) bzgl Auskunft, Löschung, Sperrung, Übertragung
- Klärung der rechtlichen Grundlage für Verarbeitung Personaldaten für internationale SEW-Lokationen

## Maßnahmen zur Gewährleistung der Compliance (6)

Bereich Organisation durch bDSB und Legal

-> überschaubarer Aufwand aber **großes Risiko** <-

- Modifikation Impressum und Datenschutzhinweis im Internetauftritt  
Kontaktdaten bDSB, Rechtsgrundlage, Widerspruchsrecht .....
- Modifikation der Verpflichtungserklärung zum Arbeitsvertrag  
Pflichten und Betroffenen-Rechte der AN.....
- Erstellung Organisationsanweisung  
Rechte und Pflichten von AG und AN, Hinweis auf Rechtsgrundlage, auf Zweckbindung,  
auf Datenminimierung und Datensparsamkeit. Gewährleistung der Datensicherheit.
- Vorgaben für Datentransfers in EU (Bindung Corporate Rules) und Drittstaaten



# Gewährleistung der toM's (Technisch-organisatorische Maßnahmen) nach Art 32

- Zutrittskontrolle ✓
- Zugangskontrolle ✓
- Zugriffskontrolle ✓
- Weitergabekontrolle ✓
- Eingabekontrolle ✓
- Auftragskontrolle ✓
- Verfügbarkeitskontrolle ✓

- Umzäunung, Pforte, Smartcard, Handvenenscanner, ...
- Firewall, Verschlüsselung, Smartcard, PC-Sperrung, ...
- Berechtigungskonzepte, Usermanagement, Passwörter, PINs, ...
- VPN-Client, Verschlüsselungen, RMFT ...
- Logging ...
- NDA-Erklärungen, AV-Verträge, Datenvernichtung nach ISO-Norm ...
- RZ-Sicherheit, Hochverfügbarkeitssysteme, Datensicherungen, ...

Zertifiziert nach ISO27001  
Permanentes ISMS



*Keine weiteren  
Aktivitäten notwendig*

## Übersicht aller Maßnahmen (1/3)

Generelle technisch-organisatorische Maßnahmen						
1	Datenschutz Prozessbeschreibung; teilweise Veröf	Erstellung eines Dokumentationsrahmens (analog ISMS). Darin werden sukzessive alle Vorgaben und Dokumente aufgenommen	Art 5 und 24	hoch	15	DSB + Unterstützung
2	Erweiterung/ Aufbau Verzeichnis von Verarbeitungstätigkeiten (Verfahrensbeschreibung)	Jedes einzelne Verfahren, bei dem personenbezogene Daten verarbeitet werden, muss nach umfangreichen Kriterien beschrieben	Art 30	hoch	40	DSB + Unterstützung
3	Erstellung Organisationsanweisung	Zum 25.5.2018 sollte eine OA erstellt werden, in der die Rechte und Pflichten von Unternehmen und Mitarbeiter angewiesen und kommuniziert werden. Nennung Rechtmäßigkeit und Transparenz der Verarbeitung, Zweckbindung, Datenminimierung und Datensparsamkeit. Entwurf durch Herrn Dr. Lachenmann	Art 5, 24, 40, 88 § 26	hoch	7	3 DSB Legal 3 1PL
4	Entwicklung eines Systems zur Datenschutz-Folgenabschätzung	Der DSB sieht diesen Punkt durch die Risikoanalyse der CI's in der CMDB abgedeckt, denn nach Art 35 (3) wird keine Verpflichtung gesehen. Erstellung Dokument mit Darstellung	Art 35	mittel	1	DSB
5	Einführung Wirksamkeitskontrollen zur regelmäßigen Überprüfung	Der bDSB schlägt hierzu einen zweijährigen Audit durch einen externen, einschlägig geschulten RA vor. Keine freiwillige Zertifizierung nach Art 42	Art 41	mittel	1	DSB
6	Anpassung/Einführung ADV-Verträge	Überprüfung und Anpassung der bestehenden (wenigen) ADV-Verträge	Art 26-28	hoch	3	2 DSB Legal 1
7	Schulungskonzept fortentwickeln / Basisschulung und fachspezifische Schulung	Im Rahmen der Erweiterung des eLearning-Moduls zum späteren Zeitpunkt (ab 2020). Zu Beginn abgedeckt durch OA	Art 39	mittel		
8	Modifizierung der Verpflichtungserklärung zum Arbeitsvertrag	Modifikation von Punkt 3 der Verpflichtungserklärung. Aufklärung über Betroffenenrechte. Für neue Arbeitsverträge. Keine Modifikation von alten Verträgen, da durch OA abgedeckt.	Art 5, 24, 32, 88 § 26	hoch	2	1PL Legal 1
9	Prozessbeschreibung Anspruchsmeldung interner und externer Betroffener. Erstellung von Standardschreiben.	Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenportabilität, Widerspruch, Vorgaben in der Verfahrensbeschreibung, Musterformulare von	Art 15-21 34-36	§ hoch	9	4 DSB Legal 5
10	Prozessbeschreibung Datenschutzvorfall	Interne Behandlung und Meldung an Aufsichtsbehörde. Nur 72 Stunden Zeit für Meldung des Vorfalls	Art 33-34	hoch	4	2 DSB Legal 2
11	Vorgaben an Drittstaatentransfers	Erstellung der Regeln, wenn personenbezogene Daten in Ländern außerhalb der EU transferiert werden müssen. ADV-Verträge als Vorlage für EURODRIVES bzgl HR-Ministamm und CRM International	Art 44-49	mittel	3	Legal
12	Mitteilung an EURODRIVES	Hinweise auf Maßnahmen in D, sowie Rechte und Pflichten in den EURODRIVES aufgrund deren lokaler Gesetzgebung. Zeichnung durch GF			1	DSB
13	Postfach bDSB anlegen	Für Datenschutzhinweise im Internet				
14	Artikel im EURODRIVER	Zur Sensibilisierung der Mitarbeiter	Art 39	niedrig	2	DSB
16	Betriebsvereinbarung Videoüberwachung	Im Dez 2017 in Absprache mit Betriebsrat. Anpassung an DSGVO			1	DSB
17	Meldung des DSB an die Aufsichtsbehörde	Zeitnah zum 25.5.2018. Gegebenenfalls bietet Aufsichtsbehörde Meldung via Internet an	Art 47 (7)			

## Übersicht aller Maßnahmen (2/3)

Maßnahmen im Bereich Vertrieb/Marketing							
100	Verfahren zur Berücksichtigung eines Widerspruchs von Kunden; insbesondere bei Abmeldung von jeglicher Werbung (Print, eMail...)	Prozessbeschreibung	Art 21	hoch	5	1 CC VB2 Legal	1 3
101	externe Aufträge an Druckerei	Absprache mit Herrn Currie CC P		niedrig			
102	Marketing Automation Tool/Lead Management (Hubspot)	Geplantes Projekt unter Führung von CC	Art 6, 7, 21	hoch			
103	Mailing-Aktionen auf Basis CRM-Kundenstamm Newsletter-Aktionen und -Tool	Automatische Abmeldung mit Speicherung Timestamp (eMail-Abmeldemechanismus). Haken zur Anmeldung zu Mailings/Newletter im CRM darf nicht manuell gesetzt werden können. Gewährleistung Double Opt-in CRM-Kundenstamm mit Speicherung Timestamp/Historie (wer/wann Eintrag erstellt wurde). Betrifft eMail, Telefon, Print. National und International. Bestandsdaten und Neueinträge. Ggf Belegverlinkung in Doxis Datenminimierung bei Anmeldung zum Newsletter (nur Mailadresse	Art 6, 7, 21	hoch	69	45 ITSS 10 ITSI 10 IP CC Legal	2 2
104	Datenschutzhinweis im Internetauftritt	Kontaktdaten bDSB, Rechtsgrundlage, Empfänger von Daten, Speicherung, Betroffenenrechte, Widerrufsrecht	Art 13	hoch	1	Legal	
105	Online Support Registrierungsprozess	Realisierung Opt in bei Anfrage für Doku per Mail, Änderung Kontaktformular, Datenminimierung, Absprache mit IP	Art 6, 7, 21	hoch	4	2 IP 2 IT	
106	Analyse Internetauftritt SEW	Zusätzliche Erläuterung, Pflichtfelder reduzieren, Entfernung Checkbox und Link auf DS-Erklärung ( bei Kontaktformularen), Datenminimierung	Art 6, 7, 21	hoch	1	CC	
107	Impressum des Internetauftritts	Angabe natürlicher Person, Rechtsgrundlage	§5 TMG	hoch	1	Legal	
108	Nutzung eTracker	Opt Out setzen, Anonymisierungsfunktion, Vertragsänderung "Auftragsdatenverarbeitung"	Art 6, 7 21	hoch	4	1 CC 3 Legal (für 106 - 108)	
109	SEW-Tracking-Funktion	Information über Tracking in Datenschutzerklärung, Schaffung Opt-out Möglichkeit, Anonymisierung IP-Adresse, Verarbeitung von Erkenntnissen über Nutzerverhalten nur nach separater Einwilligung, Datenschutzhinweis bei Versand eCodes, Prozess für Löschung, Vorgaben für Dankeschreiben; dabei Link auf eigenständige Opt Out gewährleisten, Anpassung Datenschutzerklärung	Art 6, 7, 21	hoch	23	15 IT 2 CC Legal	5 IP 1
110	eCodes Messen/Eintrittskarten	Datenschutzhinweis bei Versand eCodes, Prozess für Löschung, Vorgaben für Dankeschreiben; dabei Link auf eigenständige Opt Out gewährleisten, Anpassung Datenschutzerklärung	Art 6, 7, 21	niedrig	4	2 CC Legal IT	1 1
111	Retargeting/Remarketing Google	Opt Out gewährleisten, Anpassung Datenschutzerklärung	Art 6	hoch	1	CC mit Legal-Beratung	
112	Verwendung von Personen-Bilddaten bei Marketing	Anpassung des Formulars zur Einwilligung, Ausdrückliche Nennung der juristischen Personen, die mit den Bilddaten arbeiten dürfen, Nennung von Zweck, Präsentationsmethoden und Nutzungsform; Hinweis auf DS-Erklärung,	Art 6	hoch	2	1 CC Legal	1
113	Sponsoring-Anfragen	Aufnahme in Verfahrensverzeichnis; Datenschutzhinweis bei Anfragen; Verfahren für Löschung bei Ablehnung		niedrig	2	CC	
114	Pflege und Speicherung CRM-Kundenstamm	Aufnahme in Verfahrensverzeichnis, Aufnahme in Pflegeleitfaden: Behandlung Freitextfelder, Löschungsvorgaben, Berechtigungskonzept (vgl. hierzu auch Word-Dokument "Anforderungen Marketing an CRM")		mittel	20	3 VB2 PK 10 ITSS 5 ITSI 2 Legal	

## Übersicht aller Maßnahmen (3/3)

Maßnahmen im Bereich Human Resources						
200	Organisatorischer Datenschutz gegenüber Mitarbeitern	Die Themenbereiche Datenschutzrichtlinien, Organisationsanweisung bzw Betriebsvereinbarung, Schulungen und Einwilligung in Foto-Nutzung sind in den Ziffern	Art 5, 24, 40, 88 § 26	hoch		
201	Überprüfung bestehender Betriebsvereinbarungen	Es wird kein Ansatz gesehen, wo bestehende Betriebsvereinbarungen gegen die neue Rechtslage verstoßen könnten		gering	1	Legal
202	"who is who" im Intranet	Es wird davon ausgegangen, dass über Erwägungsgrund 48 die internationalen Zugriffe möglich sind. Offen ist die Frage, ob dafür Standardvertragsklauseln notwendig sind.	Art 5, 24, 40, 88 § 26	mittel	1	Legal
203	HR-Geschäftsprozesse und Datenanalyse aus HR (Reports)	Alle HR-Geschäftsprozesse und Gruppierungen von Auswertungen sind im Verzeichnisse mit den umfassenden Kriterien zu erfassen	Art 30	hoch	23	9 PL DSB Legal 9 5
204	Archivierung HR-Stammdaten	Prozessbeschreibung zur Gewährleistung der Ansprüche von Betroffenen (Löschung etc). Darstellung, welche HR-Daten zu löschen sind.	Art 16-20	hoch	5	2 PL Legal 3
205	Verpflichtungserklärung für Bearbeiter und Administratoren personenbezogener Daten	Neufassung als Ersatz für die bestehenden Erklärungen für Mitarbeiter in Personal und IZT	Art 39	mittel	4	2 PL 2 Legal

## Information / Kommunikation / Awareness

1. Präsentation bei GF am 28. Nov 2017 - Abstimmung Maßnahmenplan und Mittelfreigabe
2. Beauftragung Mitarbeit für Legal Dr. Matthias Lachenmann, Fa Pauly & Partner Dez 2017
3. Information der Fachabteilungen via Schreiben GF/DSB an die HAL 16. Januar 2018
4. Mitteilung an EURODRIVES durch GF/DSB 14. Februar 2018
5. Vor-Ort-Information der HAL-Bereiche und Betriebsrat durch den DSB (anhand dieser Präsentation) Februar, März und April 2018
6. Abstimmung mit SEW-USOCOME, SEW PowerSystems und diverse EURODRIVES März, April, Mai 2018
7. Artikel im EURODRIVER Mitte Mai 2018
8. Organisationsanweisung zeitnah zum 25.5.2018
9. Modifikation eLearning-Sequenz SECURITY POLICY mit Regeln zur DSGVO

## Science Fiction 1991

**Ein Beispiel: Der gläserne Konsument. Aus: „Die Woche“, Anfang 90er Jahre. Ein fiktiver Verbraucher namens Meyer findet ein Anschreiben eines ihm völlig unbekanntem Sportkonzerns in seinem Briefkasten: „... Zu Ihrem 35. Geburtstag möchten wir Ihnen als aktivem Basketball-Liebhaber ein besonderes Angebot unterbreiten - unsere neuen Qualitätsschuhe Topass. Der Einfachheit halber haben wir ein passendes Paar in Größe 44 gleich mitgeschickt. In Ihrem Homebanking-Dienst wartet ein fertig ausgefüllter Überweisungsauftrag nur noch auf das O.K. per Tastenklick. Als kleines Dankeschön für Ihre Bestellung ist der Film „Emanuelle VI“ beigelegt, der Ihnen ja noch in Ihrer privaten Sammlung fehlt... ”**

## Heute:

**“ Ihre täglichen Aktivitäten werden 24/7 überwacht und evaluiert. Was Sie einkaufen, wo Sie sich aufhalten, wer Ihre Freunde sind, wie Sie mit Ihnen interagieren, wie viele Stunden Sie mit dem Konsum von Inhalten oder Online-Spielen verbringen, welche Rechnungen und Steuern Sie bezahlen (oder nicht). Das Meiste davon passiert bereits, dank Google, Facebook, Instagram oder Gesundheits-Apps.**

**Aber was, wenn: Verhaltensmuster als negativ oder positiv bewertet werden und in einer Zahl münden, anhand der jedermann weiß, ob Sie vertrauenswürdig sind. Ihre Bewertung wird öffentlich auf einer Skala mit der kompletten Bevölkerung verglichen und benutzt, um z.B. Ihre Berechtigung für Hypotheken zu erstellen, welche Bandbreiten Sie zukünftig im Netz zugewiesen bekommen, wo Ihre Kinder zur Schule gehen dürfen, Ihre Chancen für ein Date zu definieren ... .”**

**Fiktion?**

**Aus: Big data meets Big Brother as China moves to rate its citizens**

<http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>

**Wohin geht die Reise?** Fremdbestimmung vs. Selbstbestimmung oder Die Tücken der Bequemlichkeit