enercity
positive energie

EU-Datenschutzgrundverordnung (DS-GVO)

Thomas Dorstewitz - enercity

29. SAP/NT Konferenz für Betriebs- und Personalräte (08./10.11.2016)

EU-Datenschutzgrundverordnung

EU-Datenschutzgrundverordnung

enercity
positive energie

… alles bleibt!

… aber
ANDERS!

EU-Datenschutzgrundverordnung
Betriebsrat - Motivation

Warum sollte sich der Betriebsrat mit der

EU–DatenSchutzGrundVerOrdnung
(DS-GVO)

beschäftigten?

EU-Datenschutzgrundverordnung
Betriebsrat - Motivation

… wir stehen vor einer grundlegenden Digitalisierung unseres alltäglichen Daseins, besonders auch im beruflichen Alltag:

- Vernetzung: Maschinen, Geräte, Sensoren und Menschen können sich miteinander vernetzen und können über das Internet der Dinge oder das Internet der Menschen kommunizieren.
- Informationstransparenz: Sensordaten erweitern Informationssysteme digitaler Fabrikmodelle, um so ein virtuelles Abbild der realen Welt zu erstellen.
- Technische Assistenz: Assistenzsysteme unterstützen den Menschen mit Hilfe von aggregierten, visualisierten und verständlichen Informationen. So können fundierte Entscheidungen getroffen und auftretende Probleme schneller gelöst werden. Außerdem werden Menschen bei anstrengenden, unangenehmen oder gefährlichen Arbeiten physisch unterstützt.
- Dezentrale Entscheidungen: Cyberphysische Systeme sind in der Lage, eigenständige Entscheidungen zu treffen und Aufgaben möglichst autonom zu erledigen. Nur in Ausnahmefällen, zum Beispiel bei Störungen oder Zielkonflikten, überträgt es die Aufgaben an eine höhere Instanz.

Quelle: Wikipedia

EU-Datenschutzgrundverordnung
Betriebsrat - Motivation

enercity
positive energie

Betriebsverfassungsgesetz Datenschutzfunktion des Betriebsrats	
§ 75 II	Schutz der Förderung der freien Entfaltung der Persönlichkeit der Beschäftigten
§ 80 I	Kontrolle der Einhaltung sämtlicher zugunsten der Beschäftigten bestehenden Datenschutzregelungen
§ 90	Unterrichtung und Beratung über die Auswirkungen geplanter neuer Techniken
§ 87 I Nr. 1	Mitbestimmung bei Regelungen, die die Beschäftigten allgemein zu einem Verhalten anweisen, mit dem die Erhebung, Verarbeitung oder Nutzung ihrer Daten verbunden ist.
§ 87 I Nr. 6	Mitbestimmung beim Einsatz technischer Überwachungseinrichtungen, das heißt auch bei jeder automatisierten Verarbeitung von Beschäftigtendaten mit der Möglichkeit der Leistungs-/Verhaltenskontrolle.
§ 94 I	Mitbestimmung bei formalisierter Erhebung von Beschäftigtendaten (Personalfragebögen)
§ 94 II	Mitbestimmung bei der Gestaltung von Beurteilungsgrundsätzen
§ 95 I	Mitbestimmung bei der Gestaltung von Auswahlrichtlinien

EU-Datenschutzgrundverordnung
Betriebsrat - Motivation

enercity
positive energie

Betriebsrat			
Mitbestimmung	Mitentscheidung	Kontroll- und Informationsrechte	Unterlassungsansprüche
Gestaltung des betriebsinternen Datenschutz-rechts durch Betriebsverein-barungen	… bei der Bestellung des Datenschutzbe-auftragten (§ 99 BetrVG)	gegebenenfalls unter Einschaltung interner / externer Sach-verständiger (§ 80 BetrVG)	… gegenüber nicht mitbestimmten Personaldaten-verarbeitungen

EU-Datenschutzgrundverordnung
Historie europäisches / nationales Recht

Artikel 12 (UN Menschenrechtskonvention - 1948)	Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.
Artikel 8 (Menschenrechtskonvention der EU - 4.11.1950/3.9.1953)	Schutz personenbezogener Daten (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. *Bestandteil des Rechts auf Achtung des Privatlebens ist auch das Recht auf informationelle Selbstbestimmung. Artikel 8 EMRK enthält damit auch eine rudimentäre Verpflichtung der Staaten zum Schutz der Daten seiner Bürger.*
Art. 16 AEUV	(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Das Europäische Parlament und der Rat erlassen gemäß dem ordentlichen Gesetzgebungsverfahren Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr. Die Einhaltung dieser Vorschriften wird von unabhängigen Behörden überwacht.
EGMR (1959)	Etablierung des Gerichtshofes für Menschenrechte zur Durchsetzung der Verpflichtungen aus der EU Menschenrechtskonvention.

EU-Datenschutzgrundverordnung
Historie europäisches / nationales Recht

Richtlinie 95/46/EG	**Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr„ (Datenschutzrichtlinie)**
Richtlinie 2002/58/EG (e-Privacy-Richtlinie)	**RICHTLINIE 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)**
Bundesdatenschutz-gesetz	Bundesdatenschutzgesetz (BDSG) (1. Fassung: 1.1.1979) Novellierungen: 1991, 2001 (durch EU Datenschutzrichtlinie), 2006, 2009 Weitere spezialgesetzliche Regelungen: Telekommunikationsgesetz Telemediengesetz Gesetz über den unlauteren Wettbewerb
Art. 1 DS-GVO	Gegenstand und Ziele (1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten. (2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten. (3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

EU-Datenschutzgrundverordnung … im Ergebnis

- Alle europäischen Regelungen verfolgten das Ziel, den Datenschutz insgesamt auf einem hohen Niveau in Europa zu harmonisieren!

- Dieses Ziel wurde aber insgesamt verfehlt, da die nationalen Staaten die EU-Richtlinien sehr unterschiedlich in nationales Recht umsetzen. Daher: →

- Erste Konsultationsverfahren „Gesamtkonzept zum Datenschutz“ (11.2000)

    - Ziel: EU-Datenschutzverordnung (direkt wirkendes Recht in allen EU-Staaten)

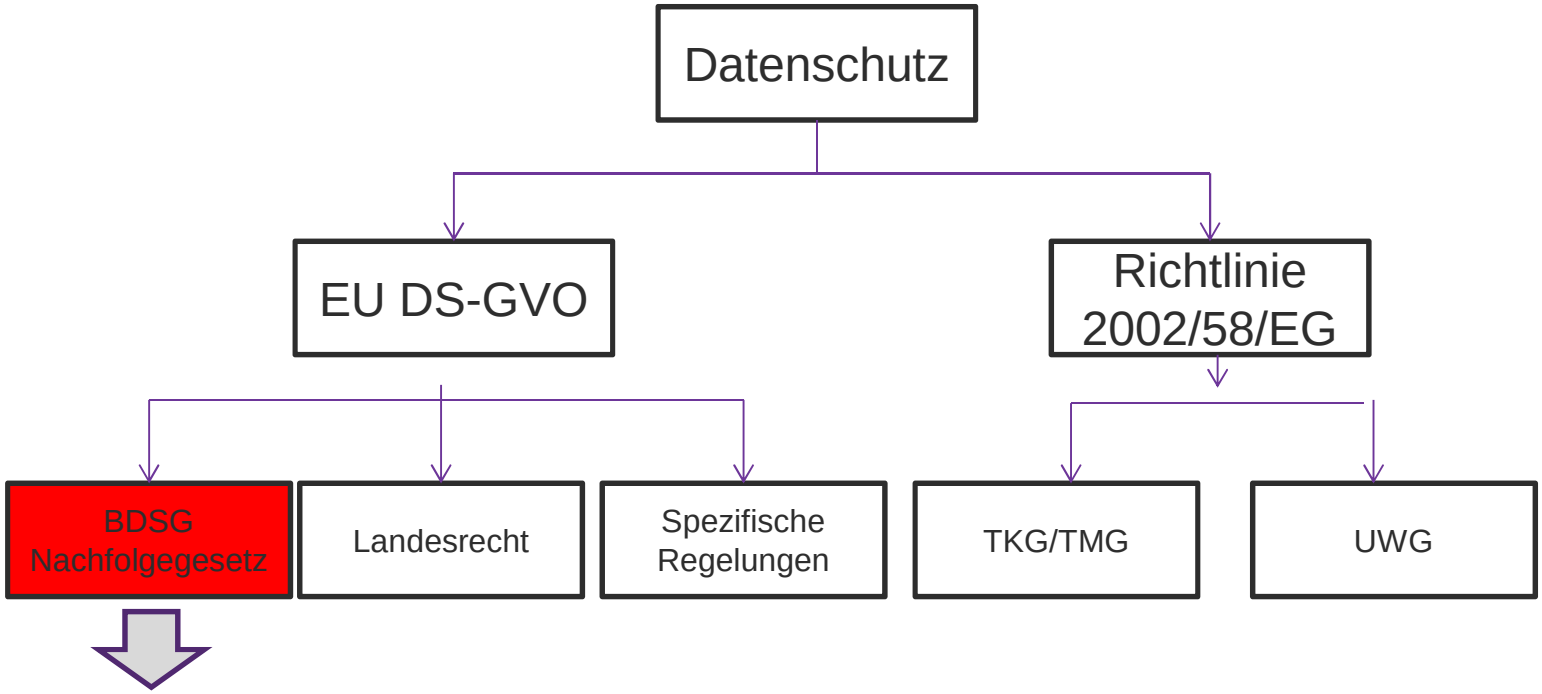
EU-Datenschutzgrundverordnung Grundbausteine

- Einheitliche Rechtsgrundlage einer Verordnung
- Eindeutige Zuständigkeit einer einzelnen Datenschutzbehörde (One-Stop-Shop)
- Einheitlich hohes Datenschutzniveau
- Berücksichtigung der Besonderheiten von Polizei und Justiz in der Rechtsarchitektur
- Besondere Aufmerksamkeit für kleinere und mittlere Unternehmen
- Ausgewogene Berücksichtigung aller Grundrechte
- Offenheit des neuen Rechtsrahmens für zukünftige technologische und wirtschaftliche Entwicklungen

EU-Datenschutzgrundverordnung Terminplan

1. Entwurf – Einbringung in das Rechtssetzungsverfahren: 25.01.2012 (Kommissionsvorschlag)
2. Weitere Vorschläge der beteiligten Parteien (Parlament, Rat)
3. Beginn/Ende der Trilog-Gespräche Juni 2015 / 15.12.2015 mit dem Ergebnis eines gemeinsamen Gesetzestextes
4. Verabschiedung durch das EU-Parlament am 14.04.2016
5. Inkrafttreten: 25.05.2016
6. Geltung ab: 25.05.2018 (Artikel 99 DS-GVO)

EU-Datenschutzgrundverordnung
Datenschutz in Europa (2016)



Öffnungsklauseln (50-60):

1. Handlungsauftrag
2. Handlungsspielraum (z.B. Artikel 88 – Beschäftigtendatenschutz)

EU-Datenschutzgrundverordnung Modernisierungsaspekte (positiv)

- Marktortprinzip
- Recht auf Vergessen werden
- Recht auf Datenübertragbarkeit
- Privacy by Design / by Default
- Verpflichtung zur Bestellung von Datenschutzbeauftragten
- Datenschutz-Folgenabschätzung (Privacy Impact Assessment) → IS Risikomanagement
- Selbstregulierung und Zertifizierung
- Effektive Durchsetzung des Datenschutzrechts
- Bessere Kontrolle über Datenübermittlungen aus der EU an Behörden und Gerichte in Drittstaaten
- Bessere Kooperation der Datenschutzaufsichtsbehörden in Europa
- Beibehaltung der Zweckbindung im bisher geltenden Umfang

EU-Datenschutzgrundverordnung Modernisierungsaspekte (negativ)

- Regelungen/Anforderungen zur Einwilligung von Betroffenen sind reduziert
- Ausdrückliche Regelung des Grundsatzes der Datensparsamkeit ist entfallen; Ersatz: Grundsatz der Datenminimierung
- Wirksame Begrenzung der Profilbildung nicht detailliert geregelt

EU-Datenschutzgrundverordnung … ausgewählte Themen …

- Öffnungsklauseln:
  - Nationale Gesetzgeber sind teilweise verpflichtet, teilweise besteht die Option, unter Beachtung der Regelungsklauseln, nationale Gesetze zu erlassen.
  - Die Bundesregierung plant ein „allgemeines Bundesdatenschutzgesetz (ABDSG, Entwurf liegt vor!)
  - Bestehende nationale Datenschutzregelungen sind hinsichtlich ihrer Konformität mit der DS-GVO zu überprüfen

EU-Datenschutzgrundverordnung … ausgewählte Themen …

- Erweiterte Dokumentations- und Nachweisregelungen. Beispiel:
  - Eine die Verarbeitung legitimierende Einwilligung ist nachzuweisen! (Art. 7 Abs. 1 DS-GVO)
  - Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO) ; künftig auch parallel Auftragsverarbeiter!
  - Datenschutz-Folgenabschätzung (Privacy Impact Assessment) und deren Ergebnisse sind vorzuhalten.
  - Datenschutzverletzungen und ergriffene Abwehrmaßnahmen sind zu dokumentieren (Art. 33, 34 DS-GVO)
  - Umfangreiche Dokumentationspflichten zur Erfüllung der Transparenzpflichten gegenüber Betroffenen (Art. 12,13,14, 15-22, 34 DS-GVO)

EU-Datenschutzgrundverordnung … ausgewählte Themen …

- Datensicherheit = Verpflichtung zur Umsetzung von technischen und organisatorischen Maßnahmen:
  - Pseudonymisierung und Verschlüsselung
  - Gewährleistung der Schutzziele: Vertraulichkeit, Integrität und Verfügbarkeit
  - Fehlertoleranz und Widerstandsfähigkeit gegenüber Störungen
  - Fähigkeit zur Wiederherstellung in der erforderlichen Zeit
  - Regelmäßiger Prozess zur Überprüfung der ergriffenen Sicherheitsmaßnahmen

EU-Datenschutzgrundverordnung … ausgewählte Themen …

- Sanktionen
  - Zivilrechtliche Haftung (Beweislastumkehr) für materielle und immaterielle Schäden
  - Haftung für Ordnungswidrigkeiten: 20.000.000 Euro oder bei Verletzung von grundlegenden Prinzipien bis zu 4 Prozent des weltweiten Konzernumsatzes (Beispiel: Einwilligung, Betroffenenrechte)

EU-Datenschutzgrundverordnung
Streiflicht: Beschäftigtendatenschutz

enercity
positive energie

- Es gibt in der DS-GVO keine zentrale Regelungsvorschrift, welche rechtgestaltenden Charakter zum Beschäftigtendatenschutz besitzt.
- Artikel 88 (155) DS-GVO sieht jedoch eine Option für den nationalen Gesetzgeber vor, den Beschäftigtendatenschutz zu regeln (Öffnungsklausel).
  - gesetzlich (→ ABDSG)
  - kollektivrechtlich (Tarifvertrag / BV)

So sieht der bisherige Entwurf des ABDSG der Bundesregierung vor, den bisherigen § 32 BDSG (Beschäftigtendatenschutz) nahezu 1:1 zu übernehmen.

EU-Datenschutzgrundverordnung
Was macht enercity?

Seit Mai 2016 AG „EU-Datenschutzgrundverordnung“

1. Kernteam
   - Beauftragter für Informationssicherheit (Leitung)
   - Organisationsberatung / -koordination
   - Personalbereich (Arbeitsrecht)
   - Datenschutzbeauftragter
   - Betriebsrat (DV-Ausschuss)

2. Erweitertes Team
   - Alle Hauptabteilungen (alle betroffen) haben Vertreter benannt

EU-Datenschutzgrundverordnung
Was macht enercity?

Arbeitspaket	Inhalt
Prozesse	Erhebung der Prozesse (Workflows & Prozessbeschreibungen) (s. u. Bemerkungen) Beispiele: Meldeprozess, Auskunftsersuchen
Datenschutzorganisation	• Erhebung der Datenschutzorganisation (s. u. Bemerkungen) • Erhebung der datenschutzrechlichen Regelungen (s. u. Bemerkungen) • Erhebung relevanter Betriebsvereinbarungen • Erhebung der datenschutzrechtlichen Aspekte in der Internen Verarbeitungsübersicht
Auftragsdatenverarbeitung	• Erhebung der Verträge zur Auftragsdatenverarbeitung (s. u. Bemerkungen) • Erhebung der Verträge zur Funktionsübertragung (s. u. Bemerkungen) • Erhebung der datenschutzrechtlichen Aspekte der mit Dienstleistungs- und Partnerverträge
TOM	• Erhebung technisch/organisatorischer Maßnahmen (§ 9 BDSG) (s. u. Bemerkungen) • Erhebung der datenschutzrechtlichen Aspekte in der Betriebsführungsdokumentation • Erhebung Löschkonzepte • Erhebung der technischen Schnittstellen zum Austausch von pers. bez. Daten (hier auch Datenübermittlung an Dritte)

EU-Datenschutzgrundverordnung
Was macht enercity?

Arbeitspaket	Inhalt
Personalmanagement	• Erhebung der datenschutzrechtlichen Aspekte in Arbeitsverträgen • Erhebung der datenschutzrechtlichen Aspekte bei Bewerbungen, etc.
Kundenmanagement	• Erhebung der datenschutzrechtlichen Aspekte in den Kundenvertäge (Lieferverträge Strom, Gas, Wasser, Wärme) • Marketing / Kundenansprache
Online-Dienste	• Internet: Erhebung der datenschutzrechtlichen Aspekte - auch das öffentliche Verfahrensverzeichnis mit berücksichtigen • Web-Portal: Erhebung der datenschutzrechtlichen Aspekte in den Web-Portalen • Intranet: Erhebung der datenschutzrechtlichen Aspekte im Intranet
… weitere Arbeitspakete bei Bedarf	• Es ergeben sich durch die DS-GVO zahlreiche Neuerungen, die im Verlauf der AG noch festzustellen und umzusetzen sind.

EU-Datenschutzgrundverordnung
Was macht enercity?

- Die einzelnen Arbeitspakete werden von „Kümmerern“ koordiniert.
- Phasenmodell:
  - Phase 1: Ist-Aufnahme (bis 30.03.2017)
  - Phase 2: Feststellen der Anpassungsbedarfe (bis 30.09.2017)
  - Phase 3: Umsetzen identifizierter Maßnahmen (bis 30.05.2018)
- Weitere Ziele:
  - Aufbau eines ganzheitlichen Datenschutzmanagements
  - Integration / Berücksichtigung ISMS
  - Zentrale Dokumentation, wo sinnvoll und möglich
  - Option: Zertifizierung (gemäß DS-GVO)

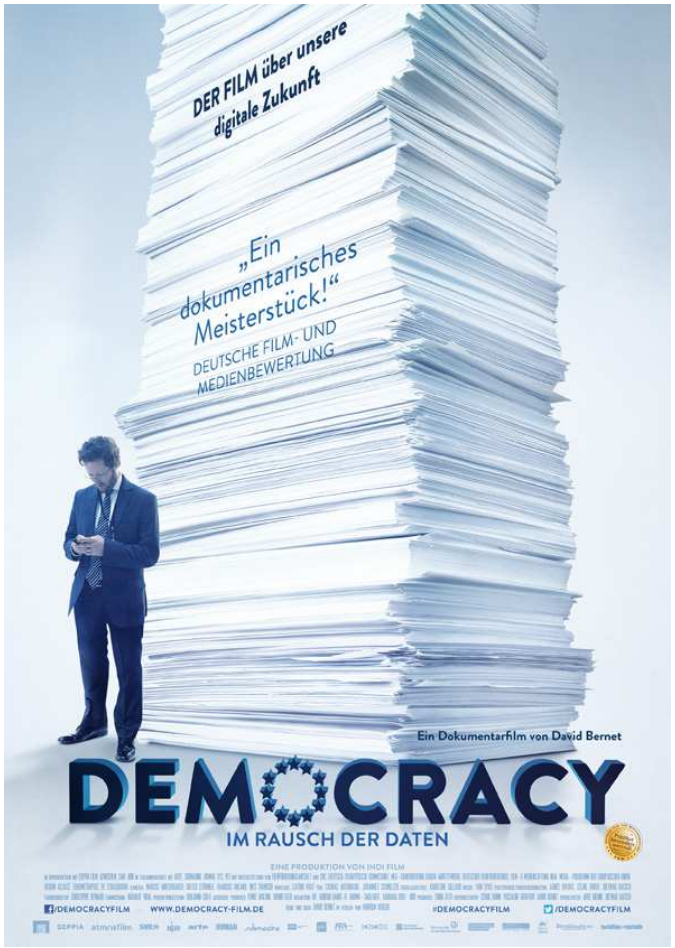
EU-Datenschutzgrundverordnung
Democracy – im Rausch der Daten

enercity
positive energie

... bis gleich im Forum!!!

Der
Dokumentationsfilm
zur
EU-Datenschutzgrundverordnung

Einblicke in die
Entstehungsgeschichte
der
EU-Datenschutzgrundverordnung
und den
„Politikbetrieb EU“



Vielen Dank
für Ihre Aufmerksamkeit!

Thomas Dorstewitz
OE 202 – Abteilung Unternehmenssicherheit
Geschäftsfeld Informationssicherheit
informationssicherheit@enercity.de

EU-Datenschutzgrundverordnung
Zu guter Letzt

https://www.menschenrechtserklaerung.de/die-allgemeine-erklaerung-der-menschenrechte-3157/

https://www.menschenrechtskonvention.eu/privatsphaere-und-familienleben-9292/

http://www.coe.int/de/web/conventions/full-list/-/conventions/rms/0900001680078b38

http://www.bpb.de/politik/hintergrund-aktuell/219563/datenschutzkonvention

https://netzpolitik.org//wp-upload/2016/09/Referentenentwurf_DSAnpUG_EU.pdf