



SACHSEN-ANHALT

Landesbeauftragter  
für den Datenschutz

# Die EU-Datenschutz-Grundverordnung – Anforderungen an die Wirtschaft 4.0

Dr. Harald von Bose

# Überblick

- Bedeutung von Datenschutz, Informationssicherheit und Informationsfreiheit für die Digitale Agenda LSA
- Rechte und Pflichten aus der Datenschutz-Grundverordnung (DS-GVO) – ein Überblick
- DS-GVO und Wirtschaft 4.0 – wie geht das?
- Informationsfreiheit – Open Data
- Forderungen an die Digitale Agenda

# Datenschutz und Informationssicherheit – Querschnittsthemen für jedes Unternehmen

- Globalisierung; Digitalisierung und Vernetzung
- Rechtslage (DS-GVO, BDSG-neu, ...) – es gibt kein belangloses Datum (Verbraucher; Beschäftigte)
- Informationssicherheit (IT-Systeme; Kritische Infrastrukturen; Geschäftsgeheimnisse)
- Datenschutz-Management (Datenschutz ist Chefsache)



# Datenschutz, Informationssicherheit und Informationsfreiheit – Querschnittsthemen für die Digitale Agenda

- **Infrastruktur /Netze** (ITN-XT, Breitbandausbau; Cloud-Systeme)
- **Wirtschaft 4.0** (Big Data; Open Data)
- **Daseinsvorsorge** (Digitales Dorf; Gesundheit 4.0)
- **E-Government** (EGovG LSA; Onlinezugangsgesetz: Portalverbund, Nutzerkonto)
- **Digitale Bildung** (Datenschutz-Management; Medienkompetenz)



# Moderner Datenschutz – Bestandteil der Digitalen Agenda 2017

- **DS-GVO:** Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 **zum Schutz natürlicher Personen** bei der Verarbeitung personenbezogener Daten, zum **freien Datenverkehr** und zur Aufhebung der Richtlinie 95/46/EG – Datenschutz-Grundverordnung – **99 Artikel und 173 Erwägungsgründe (EG)**

**Bereits in Kraft, ab dem 25. Mai 2018 unmittelbar anzuwenden**

- **E-Privacy-Verordnung** der EU  
(derzeit nur als Entwurf vorhanden, soll aber ebenfalls ab dem 25. Mai 2018 unmittelbar anzuwenden sein)
- Deutschland: Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU inkl. „**BDSG-neu**“ - verkündet am 5. Juli 2017
- **Also: jetzt auf neue Rechtslage vorbereiten!**



# Ziele der DS-GVO

- **Harmonisierung**, gleichmäßig hohes Datenschutzniveau
  - ein **einheitliches Datenschutzrecht** für in der EU tätige Unternehmen (inkl. Marktortprinzip)
  - kein „Forum-Shopping“ möglich (Datenverarbeitung in Mitgliedstaat mit geringstem Datenschutzniveau)
  - „One-Stop-Shop“; **konzentrierte Zuständigkeit** der Aufsichtsbehörden (federführende Aufsichtsbehörde am Hauptsitz des Unternehmens)
  - Stärkung des **Binnenmarktes** (wirtschaftlicher Fortschritt)
- **Modernisierung**  
Technologische Entwicklung / Globalisierung / Internet

*Frage: auch bei Big Data / Wirtschaft 4.0 ?*



SACHSEN-ANHALT

Landesbeauftragter  
für den Datenschutz

# DS-GVO:

## Prinzip des Verbots mit Erlaubnisvorbehalt

- **Art. 6 Abs. 1:** Verarbeitung ist nur rechtmäßig, wenn eine **Einwilligung** vorliegt oder eine andere in der **Vorschrift** genannte Fallgruppe (z. B. Vertrag, öffentliches Interesse, Interessenabwägung) erfüllt ist. Ansonsten ist sie verboten!
- Grundsatz gilt für
  - **einfache Datenverarbeitungen** u. **komplexe Anwendungen** wie bei Big Data oder Wirtschaft 4.0!
  - alle, die über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden, Art. 4 Nr. 1 (KMU und Großunternehmen)



## DS-GVO: weitere Prinzipien (nicht abschließend)

- **Erforderlichkeit, Datenminimierung**, Art. 5 Abs. 1 c)  
Beschränkung der Verarbeitung auf das **erforderliche Maß**, jetzt ausdrücklich in DS-GVO: Data Protection by Design/Default: Möglichkeit, mit Technik datenminimierend umzugehen
- **Zweckbindung**, Art. 5 Abs. 1 b)  
Verarbeitung nur für **festgelegte, eindeutige Zwecke**; Zweckänderung ohne Einwilligung nur, wenn Zweckänderung mit Ursprungszweck vereinbar (Privilegierung für im öffentlichen Interesse liegende Archiv-, wissenschaftliche oder historische Forschungs- und Statistikzwecke, Art. 89)
- **Transparenz**, Art. 5 Abs. 1 a), 12 ff.  
Informationspflichten und Auskunfts-, Berichtigungs-, Lösungsrechte
- **Sicherheit der Verarbeitung** (Datensicherheit), Art. 32
- **Unabhängige Datenschutzaufsicht**, legt Datenschutz-Vorschriften im Zusammenwirken mit Europäischem Datenschutzausschuss aus und verfügt jetzt über Abhilfebefugnisse auch gegenüber Behörden, Art. 51 ff.



# DS-GVO: Data Protection by Design & by Default

(Datenschutz durch Technikgestaltung & datenschutzfreundliche Voreinstellungen)

- **Ziel:** Gestaltung von Systemen und Diensten von Anfang an durch technischen Datenschutz und mit möglichst datenschutzkonformen Voreinstellungen (**Art. 25, EG 78**)
- **Inhalt:** Pflicht zur Implementierung techn. und org. Maßnahmen zur Umsetzung der DS-GVO, z. B. Datenminimierung, frühestmögliche Pseudonymisierung, Transparenz (**Art.32**)
- **Maßstab:** Stand der Technik, Implementierungskosten, mit der Verarbeitung verbundene Risiken (Senkung des Risikos bei Nutzung europäischer Dienstleister – „Trusted Cloud“), Zertifizierung möglich
- **Zielgruppe:** **Verantwortlicher** (auch **Auftragsverarbeiter**), indirekt aber auch Hersteller von IT-Systemen (**Marktchance!**)



SACHSEN-ANHALT

Landesbeauftragter  
für den Datenschutz

# DS-GVO: neue/erweiterte Betroffenenrechte

- **Recht auf Vergessenwerden, Art. 17 Abs. 2**  
Hat der Verantwortliche zu löschende Daten zuvor öffentlich bekannt gemacht, trifft er angemessene Maßnahmen, um die Verantwortlichen, die diese Daten verarbeiten, zu informieren, dass die betroffene Person Löschung verlangt hat
- **Recht auf Datenübertragbarkeit, Art. 20**  
Daten müssen in einem strukturierten, gängigen und maschinenlesbaren Format bereitgestellt werden, wenn Verarbeitung automatisiert erfolgt und auf Einwilligung oder Vertrag nach Art. 6 Abs. 1b) beruht
- **Widerspruchsrecht, Art. 21**  
Recht besteht in besonderen Situationen bei Datenverarbeitungen, die auf Interessenabwägung beruhen (auch Profiling); Folge des Widerspruchs: keine Weiterverarbeitung, Ausnahme: zwingende Gründe oder Rechtsverteidigung
- **Erweiterte Informationspflichten des Verantwortlichen, Art. 13, 14**  
Z. B. über bestimmte Betroffenenrechte und Beschwerderecht bei der Aufsichtsbehörde



# DS-GVO: Dokumentations- und Nachweispflichten (1)

- **Verzeichnis von Verarbeitungstätigkeiten, Art. 30**

Pflicht für Verantwortlichen (Abs. 1) und Auftragsverarbeiter (Abs. 2) mit jeweils unterschiedlichen Inhalten

- gilt für **alle Verarbeitungen** nach DS-GVO!
- muss **nicht mehr jedermann verfügbar gemacht** werden, aber
- auf Anforderung der **Aufsichtsbehörde zur Verfügung gestellt** werden
- Form: schriftlich oder elektronisch

*- Vordruck demnächst auf der Homepage des LfD -*

- **kein Verzeichnis erforderlich** bei Unternehmen, die **weniger als 250 Mitarbeiter** beschäftigen, **sofern** die Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Person birgt, sie nur gelegentlich erfolgt oder nicht besondere Kategorien personenbezogener Daten oder Straftaten einschließt



## DS-GVO: Dokumentations- und Nachweispflichten (2)

- **Einhaltung der Grundsätze** der Verarbeitung:  
Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit (**Rechenschaftspflicht**), Art. 5 Abs. 2
- Umsetzung **geeigneter technischer und organisatorischer Maßnahmen**, um sicherzustellen und den **Nachweis** zu erbringen zu können, dass die Verarbeitung gemäß der DS-GVO erfolgt, Art. 24 Abs. 1
- Nachweispflicht bei **Auftragsverarbeitung**, Art. 28
- Dokumentationspflicht bei **Verletzungen** des Datenschutzes, Art. 33 Abs. 5
- Einhaltung der DS-GVO bei erforderlicher **Datenschutz-Folgenabschätzung**, Art. 35 Abs. 7 Buchst. d)
- Garantien bei **Drittstaatenübermittlungen**, Art. 46 ff.



# DS-GVO: Datenschutz-Folgenabschätzung (DSFA)

- Durchführung erforderlich, wenn Art, Umfang, Umstände und Zweck der Verarbeitung **voraussichtlich ein hohes Risiko** für die persönlichen Rechte und Freiheiten zur Folge haben, Art. 35 Abs. 1
- Hohes Risiko liegt insbesondere nahe bei **umfangreichen, vernetzten Verarbeitungen** wie bei Wirtschaft 4.0 und Big Data. Art. 35 Abs. 3 nennt Regelbeispiele, die nicht abschließend sind, z. B. Abs. 3 c: „systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche“.
- Art. 35 Abs. 7 gibt Mindestinhalte der DSFA vor (ähnlich wie bisherige Vorabkontrolle)
- Ggf. ist **Standpunkt der betroffenen Personen** oder ihrer Vertreter zur beabsichtigten Verarbeitung einzuholen (Art. 35 Abs. 9) – immer ratsam bei umfangreichen Verarbeitungen
- Besteht im Ergebnis der DSFA ein **hohes Risiko** für Betroffene, ist **vor** der Verarbeitung die **Aufsichtsbehörde zu konsultieren**, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, Art. 36 Abs. 1
  - *Art.-29-Gruppe erstellt ein Working Paper zur Frage, wann eine DSFA durchzuführen ist – später Listen der Aufsichtsbehörden -*



# DS-GVO: betrieblicher Datenschutzbeauftragter (bDSB)

- Ist gemäß **Art. 37** zu benennen, wenn **Kerntätigkeit**
  - aus Verarbeitungsvorgängen besteht, die eine **regelmäßige und systematische Überwachung** erforderlich machen
  - in der umfangreichen Verarbeitung **besonderer Kategorien** von personenbezogenen Daten (Art. 9) oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht
- **Achtung: § 38 Abs. 1 BDSG-neu** sieht ergänzend vor: Benennung bDSB zusätzlich erforderlich, wenn
  - in der Regel **mindestens 10 Personen** ständig mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind
  - oder eine **Datenschutz-Folgenabschätzung** erforderlich ist
  - oder personenbezogene Daten **geschäftsmäßig zum Zweck der Übermittlung**, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden



# Mögliche Folgen von Verstößen gegen die DS-GVO

- Aufsichtsbehördliche **Untersuchungen**, z. B. aufgrund eigener Erkenntnisse oder Beschwerden betroffener Personen
- Aufsichtsbehördliche **Abhilfeanordnungen**, z. B. die Anweisung, dem Antrag einer betroffenen Person zu entsprechen, oder das Verbot der Verarbeitung, Art. 58 Abs. 2 c), f)
- Wirksame, verhältnismäßige und abschreckende **Geldbußen** i. H. v. bis zu **20 Mio. EUR** oder **4%** des gesamten weltweit erzielten Jahresumsatzes, Art. 83
- Erfolgreiche **Klagen** von betroffenen Personen oder Verbänden, Art. 80 Abs. 1 und 2 (§ 2 Abs. 2 Nr. 11 UKlaG)



# Wann ist die DS-GVO bei Wirtschaft 4.0 und Big Data zu berücksichtigen?

- **„Wirtschaft 4.0“**: intelligente, internetgestützte Herstellung von Produkten mit (branchen-)übergreifendem Datenaustausch
- **„Big Data“**: große Datenmengen, die u.a. aus Bereichen wie Internet und Mobilfunk, Finanzindustrie, Energiewirtschaft, Gesundheitswesen und Verkehr und aus Quellen wie intelligenten Agenten, sozialen Medien, Kredit- und Kundenkarten, Smart-Metering-Systemen, Assistenzgeräten, Überwachungskameras sowie Flug- und Fahrzeugen stammen und die mit speziellen Lösungen gespeichert, verarbeitet und ausgewertet werden.
- Quelle für Big Data ist auch **„Open Data“**: *proaktive* Zurverfügungstellung staatlicher Informationen, *kostenfrei* und in *maschinenlesbaren* Formaten
- **Wann ist die DS-GVO bei Wirtschaft 4.0 und Big Data zu beachten?**  
Immer dann, wenn die **Daten personenbezogen** oder **personenbeziehbar** sind – dies gilt auch, wenn der Personenbezug erst durch Verknüpfung von Daten hergestellt wird.



# Dürfen personenbezogene Daten zu Zwecken der Wirtschaft 4.0/ des Big Data verarbeitet werden? (1)

## Ja, wenn

- die betroffene Person freiwillig, informiert, unmissverständlich **eingewilligt** hat (Art. 7, EG 32). Bei besonderen Kategorien personenbezogener Daten (z. B. Gesundheitsdaten) ausdrückliche Einwilligung erforderlich; hier keine Einwilligung erforderlich, wenn Daten von betroffener Person offensichtlich öffentlich gemacht wurden (Art. 9 Abs. 2e)  
**Problem:** ggf. umfangreiche Erklärungen notwendig bei Vielzahl von Zwecken, Zwecke zum Zeitpunkt der Erhebung noch nicht bestimmt, nicht Einwilligende sind ausgeschlossen, Einwilligung jederzeit widerrufbar  
**oder**
- die Anwendung zur Wahrung der **berechtigten Interessen** des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die **Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person** überwiegen (Art. 6 Abs. 1f)  
**Problem:** Interessen der betroffenen Person können überwiegen (insbes. bei Minderjährigen, Beschäftigten, Profiling, Veröffentlichung)



# Können personenbezogene Daten zu Zwecken der Wirtschaft 4.0/ des Big Data verarbeitet werden? (2)

## oder

- im Falle der Weiterverarbeitung deren Zweck **mit dem ursprünglichen Zweck vereinbar** ist (Art. 5 Abs. 1b, 6 Abs. 4)

Die Weiterverarbeitung im öffentlichen Interesse liegender Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt nicht als unvereinbar mit dem ursprünglichen Zweck

**Problem:** häufig nur begrenzte Anwendungen möglich

## und

- die Verarbeitung personenbezogener Daten für den Zweck **erforderlich** ist  
**Problem:** Verarbeitung muss auf das notwendige Maß beschränkt sein (Art. 5 Abs. 1c)
- die Voraussetzungen **nachgewiesen** und **dokumentiert** werden (Art. 5 Abs. 2)
- die **Betroffenenrechte** gewährleistet werden (Art. 12 – 20)



# Missachtet die DS-GVO die neuen Geschäftsmodelle?

- **These:** DS-GVO missachtet die neuen Geschäftsmodelle:  
Big Data i.V.m. Künstlicher Intelligenz und Wirtschaft 4.0:
  - Wie passen Erfordernisse der Einwilligung, Datensparsamkeit, und Zweckbindung mit Wirtschaft 4.0/Big Data zusammen?
  - Datenschatz statt Datenschutz!
  - Neue „Datensouveränität“!
  - Maschine und Algorithmen anstelle des Menschen?
- **Gegenthese/Lösungen:** Datenschatz **mit** Datenschutz!
  - sachbezogene Informationen (Logistik) – aber: Informationssicherheit beachten
  - Eigentumsrecht an Daten? Ökonomisierung der Daten?



- Ergänzend: Wettbewerbsrecht; Haftungsrecht
  - Verbindung von Recht und Technik in der Datenschutz-Folgenabschätzung gemäß DS-GVO
  - i. V. m. Data Protection by Design (Datenminimierung, Anonymisierung, Pseudonymisierung) (**Marktchance**)  
*Problem bei Anonymisierung: Re-Identifizierung!*
  - Künstliche Intelligenz (intelligente Privatsphäre-Assistenten; Verbraucher-Datenportale) (**Marktchance**)
  - Transparenz der Algorithmen
- 
- **Verfassungsrechtlicher Einwand**: Verbot der zwangsweisen Registrierung des Menschen in seiner ganzen Persönlichkeit auch mittels anonymer Daten und Verbot der Totalüberwachung (Menschenwürde und Freiheit der Persönlichkeit)



# Datenschutz – Was gehört in die Digitale Agenda?

- **Beratungsprogramme**, die es KMU ermöglichen, aktuelle Expertisen zur **Informationssicherheit** zu erhalten
- **Förderprogramme**, die insbes. KMU für DS-GVO und BDSG-neu fit machen (Förderung der Schulung von bDSB und Mitarbeitern in den Unternehmen)
- **Einbeziehung** des **LfD** in **Partnernetzwerke** und **Digitalisierungszentren** (mit Wirtschaft, Wissenschaft, Kammern, Verbänden)
- **Personell** stärker ausgestattete **Datenschutzaufsichtsbehörde**, die Unternehmen in Sachsen-Anhalt umfassender beraten kann (proaktiver Datenschutz!)
- Regionale Innovationsstrategie Sachsen-Anhalt 2014-2020 anpassen
- **Ganzheitliche Entwicklung**: Wirtschaft 4.0 verlangt nach einer Verwaltung 4.0 – **beim E-Government muss das Land aufholen!**
- **Datenschutz** und **Informationssicherheit** müssen als **Vertrauens- und Erfolgsfaktoren** und **Wettbewerbsvorteile** begriffen werden
- **Datenschutz** muss **im Beirat** zur digitalen Agenda angemessen vertreten sein
- **Beirat** sollte neben Informations- auch **Steuerungsbefugnisse** haben



# Informationsfreiheit – Was gehört in die Digitale Agenda?

- **E-Government-Gesetz** und Einführung der **elektronischen Akte** als Voraussetzung für Open Data und Open Government (Bürgerbeteiligungsportal)
- **Transparenzgesetz** mit Open-Data-Regelungen (LT-Beschluss vom 4. Mai 2017)
- Ausbau des Landesportals zu einem **Informationsregister** unter Einbeziehung der Kommunen bis zum 31. Dezember 2018 (gemäß den Prinzipien „Open Data by Design“ und „Open Data by Default“)
- Beteiligung am bundesdeutschen Portal „**govdata**“
- **Förderprogramme** für Unternehmensgründungen im Bereich von Open Data
- **Bedarfsermittlung**, welche Daten der Wirtschaft vorrangig zur Verfügung gestellt werden sollen
- Fortentwicklung der Strategie Sachsen-Anhalt digital 2020 zu einer umfassenden **E- und Open-Government-Strategie**



# Erfolgsfaktoren für Sachsen-Anhalt

## Moderne digitale Strategie:

- ganzheitlich
- nachhaltig – mit prioritären Maßnahmen
- verbindlich
- vernetzt
- **datenschutzkonform**
- Digitalisierung als Mittel zum Zweck – digitaler Aufbruch als politisches Thema
- neue Verwaltungs- und Unternehmenskultur – Bildung als Thema der Digitalisierung

## Maximen des Staates:

Vertrauen – Verantwortung – Verlässlichkeit/Widerspruchsfreiheit



SACHSEN-ANHALT

Landesbeauftragter  
für den Datenschutz

# Abschlussfragen

- Gibt es bei den Förderansätzen in Sachsen-Anhalt „weiße Flecken“?
- Was ist mit analogen „Oasen“?
- Verbot der Diskriminierung: Wie wird (demokratische) Teilhabe für Personen gewährleistet, die sich nicht „digitalisieren“?
- Müssen alle Lebensbereiche digitalisiert werden? Was muss wirklich durch Algorithmen gesteuert werden? Welche Steuerungen sollten dem Menschen vorbehalten bleiben? Privatheit im 21. Jahrhundert anstelle von Politik und Recht nur noch durch Technik und Ethik?

*„Die Menschheit selbst ist eine Würde; denn der Mensch kann von keinem Menschen (weder von anderen noch so gar von sich selbst) bloß als Mittel, sondern muss jederzeit zugleich als Zweck gebraucht werden und darin besteht eben seine Würde...“*

(Immanuel Kant, Die Metaphysik der Sitten, 1797)



# Vielen Dank für Ihre offene Aufmerksamkeit!

Weitere Informationen:

<https://datenschutz.sachsen-anhalt.de/datenschutz-sachsen-anhalt/>

<https://informationsfreiheit.sachsen-anhalt.de/informationsfreiheit-sachsen-anhalt>

Landesbeauftragter für den Datenschutz Sachsen-Anhalt  
Geschäftsstelle und Besucheradresse: Leiterstraße 9, 39104 Magdeburg  
Postadresse: Postfach 1947, 39009 Magdeburg

poststelle@lfd.sachsen-anhalt.de

Telefon: 0391 81803-0  
Freecall: 0800 9153190 (nur über Festnetz)  
Telefax: 0391 81803-33



SACHSEN-ANHALT

Landesbeauftragter  
für den Datenschutz