SACHSEN-ANHALT
Landesbeauftragter
für den Datenschutz

EU-Datenschutz-Grundverordnung – Anforderungen an den Mittelstand beim Planen und Bauen mit Building Information Modeling

Dr. Harald von Bose

Agenda

- Grundlagen des neuen Datenschutzrechts
- Rechte und Pflichten aus der Datenschutz-Grundverordnung (DS-GVO) – ein Überblick
- Dokumentationspflichten
- Technische und organisatorische Maßnahmen
- DS-GVO und BIM – wie geht das in rechtlicher und technischer Hinsicht?
- Ausblick: DS-GVO contra Big Data und KI?

Vorherige Rechtsgrundlage

Richtlinie 95/46 EG

- Problematische Aspekte laut Europäischer Kommission (Mitteilung vom 04.11.2010) u. a. in den Bereichen:
  - Beherrschung der Auswirkungen neuer Technologien (1998 ging Google online, seit 2004 gibt es Facebook)
  - Binnenmarktdimension des Datenschutzes: uneinheitliches Niveau
  - Globalisierung und internationale Datentransfers
  - institutioneller Rahmen zur Rechtsdurchsetzung

Jetzige Rechtsgrundlage

Lösung:

„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)“

Weitere Regelungen zur Anpassung an die DS-GVO

- **Europäische** Ebene
  Entwurf einer **Verordnung über Privatsphäre und elektronische Kommunikation (ePrivacy-Verordnung)**
  (http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017PC0010&from=DE)
- **Bundes**ebene
  „Datenschutz-Anpassungs- und Umsetzungsgesetz EU - DSAnpUG-EU“ (BGBl. I Nr. 44 v. 5.7.2017, S. 2097);
  darin enthalten: **BDSG 2018**, Anpassung von zahlreichen **spezialgesetzlichen Regelungen**
  (weiteres „Omnibusgesetz“ geplant)
- **Länder**ebene
  - Anpassung der **Landesdatenschutzgesetze**
  - Anpassung zahlreicher **spezialgesetzlicher Regelungen**

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 von Unternehmen)
  - EU-Kommissarin Jourova: Unternehmen sparen jährlich 2,3 Mrd. €
  - Stärkung des Binnenmarktes
- Modernisierung (Berücksichtigung Globalisierung/ Internet/ Big Data, Wirtschaft 4.0 (z.B. Building Information Modeling))

Schutzgut: Personenbezogene Daten (Art. 4 Nr. 1)

…"sind alle Informationen, **die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen**; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Onlinekennung oder zu einem oder mehreren Merkmalen… identifiziert werden kann"

z. B. : Name, Geburtsdatum, Familienstand, Aussehen, körperliche Merkmale, Adresse, Kontaktdaten, Standortdaten, Vermögensangaben, Bankverbindung, Scorewert, Zeugnisse, Ausbildung, Beruf, Verhaltensweisen, individuelle Leistungen, Interessen, Kaufverhalten, Vereins- oder Unternehmens-zugehörigkeit…

Schutzgüter des Datenschutzes sind nicht das Urheberrecht oder Betriebsgeheimnisse!

Welche personenbezogenen Daten können im Rahmen des BIM anfallen?

- **Betroffene Personen**
  Bauherren, Ingenieure, Statiker, Architekten, Bauleiter, Zeichner, Handwerker, Property- und Facility-Manager sowie *Beschäftigte der beteiligten Unternehmen*

- **Einzeldaten**
  Kontaktdaten, Qualifikationen und Spezialisierungen der Projektbeteiligten, Adressen, Foto- und Filmaufnahmen von Eigentum, Standortdaten, *Projekt- und Kalendereinträge*, …

Verbot mit Erlaubnisvorbehalt

Verarbeitung nur zulässig, wenn eine der **folgenden Fallgruppen** nach Art. 6 Abs. 1 erfüllt ist:

- **Einwilligung**
- **Vertrag** ⟶ **BIM**
- **Rechtliche Verpflichtung**
- Lebenswichtige Interessen
- Öffentliches Interesse/hoheitliche Aufgaben
- **Interessenabwägung**: berechtigtes Interesse ./. schutzwürdiges Interesse (unter besonderer Berücksichtigung der Rechte des Kindes, „Kind“ meint hier alle nach deutschem Recht Minderjährigen)

Erlaubnis zur Verarbeitung personenbezogener Daten

Personenbezogene Daten können verarbeitet werden:

- zur **Erfüllung eines Vertrages mit dem Betroffenen**, Art. 6 Abs. 1 S. 1 **b)**
  - alle Daten, die zur Durchführung vorvertraglicher Maßnahmen erforderlich sind (z. B. Name und Anschrift für Kostenvoranschlag)
  - alle Daten, die zur **Erfüllung eines Vertrages** erforderlich sind, Art. 6 Abs. 1 S. 1 b) (i. d. R. Name, Anschrift, Leistungsdetails)

- zur **Wahrnehmung berechtigter Interessen**, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten des Betroffenen überwiegen, Art. 6 Abs. 1 S. 1 **f)**
  - Nutzung der Daten zur Direktwerbung kann „in Maßen“ zulässig sein, soweit kein Widerspruch vorliegt (Art. 21 Abs. 2), Werbung per E-Mail erfordert Einwilligung (§ 7 Abs. 2 Nr. 3 UWG)

Weitere Grundsätze und Prinzipien

Art. 5, 12 ff, 25, 32, 51 ff

- **Erforderlichkeit, Angemessenheit, Datenminimierung**
  Beschränkung der Verarbeitung auf das **erforderliche Maß**, jetzt ausdrücklich in DS-GVO: data protection by design/ by default = Möglichkeit, mit Technik datenminimierend umzugehen
- **Zweckbindung**
  Verarbeitung nur für **festgelegte, eindeutige Zwecke**; Zweckänderung ohne Einwilligung nur wenn diese mit Ursprungszweck vereinbar (Privilegierung für im öffentlichen Interesse liegende Archiv-, wissenschaftliche oder historische Forschungs- und Statistikzwecke, Art. 89)
- **Transparenz**
  Informationspflichten und Auskunfts-, Berichtigungs-, Löschungsrechte
- **Rechenschaftspflicht**
- **Sicherheit der Verarbeitung**
- **Unabhängige Datenschutzaufsicht** mit Abhilfebefugnissen, jetzt auch gegenüber Behörden, inkl. Kammern (Art. 58 Abs. 2)

Was bedeuten die Grundsätze für BIM?

- Nur die Daten verarbeiten, die **für die Zweckerreichung erforderlich sind**, und Zugriffsrechte der Beteiligten auf das für Ihre Aufgabe erforderliche Maß beschränken
  - sollte schon bei der Beschaffung der Software berücksichtigt werden (data protection by design) -
- Zweck BIM: **Planung, Ausführung, Bewirtschaftung von Bauwerken** mit Hilfe einer unternehmensübergreifend genutzten Software
  Zweck ist nicht die Überwachung der Beschäftigten!
- Betroffene Personen müssen über die Verarbeitung ihrer Daten **informiert** sein
- Datensicherheit siehe Folien Nr. 18-20

Protokollierung / Nutzung von Beschäftigtendaten

- Die Zwecksetzung von BIM wird es erforderlich machen, eine **Fülle von Arbeitsschritten- und Ergebnissen**, die einzelnen Mitarbeitern zugeordnet werden können, automatisiert zu protokollieren.
- Diese mitarbeiterbezogenen Daten dürfen protokolliert und genutzt werden, soweit dies **zur Durchführung des Beschäftigtenverhältnisses erforderlich** ist, § 26 BDSG 2018. Erforderlich ist die Verarbeitung, soweit sie für die Planung, Ausführung und Bewirtschaftung im Rahmen des BIM benötigt werden.
- Die Nutzung der Daten des Beschäftigten, die durch die BIM-Software gespeichert werden, muss **verhältnismäßig** sein. Eine Verwendung zu Kontrollzwecken ist nur begrenzt zulässig, z. B.
  - bei **stichprobenartiger Qualitätskontrolle** oder
  - wenn sich aus konkreten Tatsachen der Verdacht einer **Straftat** oder einer anderen **schwerwiegenden Pflichtverletzung** ergibt.

  Ein unverhältnismäßiger Überwachungsdruck (z. B. durch Vollkontrolle) ist zu vermeiden.

Betroffenenrechte natürlicher Personen

- **Erweiterte Informationspflichten, Art. 13, 14**
  Z. B. über Betroffenenrechte und Beschwerderecht bei Aufsichtsbehörde
- **Recht auf Auskunft, Art. 15** – auf Antrag
- **Recht auf Berichtigung, Art. 16**
- **Recht auf Löschung, Art. 17 Abs. 1**
  Daten sind **unverzüglich zu löschen**, wenn sie z. B. für den Zweck der Erhebung nicht mehr notwendig sind oder unrechtmäßig verarbeitet wurden

  (Neues Recht auf Vergessenwerden, Art. 17 Abs. 2)
- **Recht auf Einschränkung der Verarbeitung, Art. 18**
- **Widerspruchsrecht, Art. 21**, z. B. bei DV infolge Interessensabwägung

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

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

(Vordruck auf Homepage des LfD)

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	

Meldepflicht des Verantwortlichen bei Datenschutzverletzungen an Aufsichtsbehörde, Art. 33, 34

- Meldepflicht besteht, wenn Verletzung zur Vernichtung, zum Verlust, zur Veränderung, zur Offenlegung, zum Zugang verarbeiteter Daten führt (gilt für **alle Datenarten**)
- **Auftragsverarbeiter** meldet dem Verantwortlichen
- Erfolgt Meldung nicht binnen **72 Stunden**, ist deren Verzögerung zu begründen
- **Inhalt**: Art der Verletzung, Kategorien und Zahlen der betroffenen Personen und Datensätze, bDSB, wahrscheinliche Folgen, Abwehrmaßnahmen
- Meldepflicht **entfällt**, wenn Verletzung „**nicht zu einem Risiko** für die Rechte und Freiheiten einer natürlichen Person führt."
  z. B.: abhanden gekommener Datenträger ist verschlüsselt gemäß Richtlinie BSI (derzeit AES 256 Bit)
- Besteht ein **hohes Risiko**, so ist unverzüglich die **betroffene Person zu benachrichtigen**
  (Ausnahme: Daten mittlerweile für Unbefugte unzugänglich, Risiko besteht nicht mehr, Benachrichtigung unzumutbar (dann aber öffentliche Bekanntmachung))
- Meldeformular: http://lsaurl.de/DSVerletzung

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Artikel 25

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

Sicherheit der Verarbeitung, Art. 32 Abs. 1 (1)

Unter Berücksichtigung

- des **Stands der Technik**
- der (Implementierungs-)**Kosten**,
- der **Art**, des **Umfangs**, der **Umstände** und des **Zwecks** der Verarbeitung
- der **Eintrittswahrscheinlichkeit** und **Schwere** des **Risikos** für Rechte und Freiheiten natürlicher Personen

treffen der Verantwortliche und der Auftragsverarbeiter **technische und organisatorische Maßnahmen**, die dem **Risiko** angepasstes **Schutzniveau** gewährleisten

Sicherheit der Verarbeitung, Art. 32 Abs. 1 (2)

Diese Maßnahmen schließen **unter anderem** Folgendes ein:

a) die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten, z. B.: Verschlüsselung bei Datenübermittlungen mit aktuellem Verschlüsselungsprotokoll, mind. TLS 1.2

b) **Sicherstellung** der **Vertraulichkeit**, **Integrität**, **Verfügbarkeit** und **Belastbarkeit** der Systeme und Dienste

c) (rasche) Wiederherstellung der **Verfügbarkeit** und den **Zugang** zu personenbezogenen Daten bei einem **physischen** oder **technischen** Zwischenfall

d) ein **Verfahren** zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der **Sicherheit** der Verarbeitung.

Cloud Computing

- Nach Möglichkeit sollten Daten in der Cloud **pseudonymisiert** bzw. **verschlüsselt** gespeichert werden.
- Es sollte ein Unternehmen mit **Sitz und Speicherort in der EU** bevorzugt werden
- Eine Speicherung **außerhalb der EU** ist nur zulässig, sofern
  - ein **Angemessenheitsbeschluss** der EU-Kommission vorliegt (Art. 45)
  - geeignete **Garantien**, z. B. verbindliche unternehmensinterne Datenschutzregelungen (Art. 46), oder
  - **Ausnahmen für bestimmte Fälle**, z. B. ausdrückliche Einwilligung (Art. 49), vorliegen

Auftragsverarbeitung, Art. 28

- **Fälle**: z. B. reine Gehaltsabrechnung, Software-Anbieter inkl. Cloud-Computing, Rechenzentren, Datenträgerentsorgung;
  nicht: Steuerberatung, Rechtsvertretung, Ingenieurleistungen
- **Vertrag** zwischen dem Verantwortlichen und dem Auftragnehmer, Art. 28 Abs. 3
- EU-Kommission oder Aufsichtsbehörden können **Standardvertragsklauseln** für die Auftragsverarbeitung genehmigen, Art. 28 Abs. 7, 8
- **Verhaltensregeln und Zertifizierungen** können Bestandteil ausreichender Garantien des Auftragsverarbeiters für die Einhaltung der DS-GVO und für den Schutz von Rechten der Betroffenen sein, Art. 28 Abs. 1, 5
- Bei Pflichtverletzung **haftet** jetzt auch der **Auftragsverarbeiter** für **Schäden**, Art. 82 Abs. 1, 2, 4

Voraussetzungen bei gemeinsamer Verarbeitung, Art. 26

Mehrere Verantwortliche (Unternehmen, Bauherr) sind gemeinsam für die Verarbeitung verantwortlich, wenn sie **gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen**. Eine gemeinsame Verarbeitung kann vorliegen, wenn einzelne Beteiligte für bestimmte Teile bzw. Phasen einer Verarbeitung getrennt verantwortlich sind, jedoch die Daten über eine gemeinsame Plattform zusammengetragen werden. Dies kann bei BIM nahe liegen, es sei denn, ein Unternehmen ist hauptverantwortlich und gibt einseitig Zwecke und Mittel vor.

Folgen bei gemeinsamer Verarbeitung, Art. 26

- **Übermittlungen** personenbezogener Daten von einem Unternehmen zum anderen erfordern auch bei gemeinsamer Verarbeitung eine Rechtsgrundlage, nach Art. 6
- Gemeinsam Verantwortliche müssen in transparenter Weise festlegen, **wer von ihnen welche in der DS-GVO geregelten Verpflichtungen erfüllt**, insbesondere die Betroffenenrechte und Informationspflichten nach Art. 13 und 14 (Beschreibung des Zusammenwirkens und der Rollen der Beteiligten)
- Jeder der Verantwortlichen **haftet** im Falle rechtswidriger Verarbeitung für den gesamten Schaden, sofern er nicht sein fehlendes Verschulden nachweisen kann, Art. 82
- Soweit aus der gemeinsamen Verantwortlichkeit hohe Risiken erwachsen, ist eine **Datenschutz-Folgenabschätzung** erforderlich

Erfordert BIM eine Datenschutz-Folgenabschätzung (DSFA)? (1)

Die DSFA ist eine **risikobezogene Pflicht** des für die Verarbeitung Verantwortlichen

- 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
- Art. 35 Abs. 3 nennt Situationen, die eine DSFA erfordern (z. B. Abs. 3 Buchst. c): „systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche“)
- Die Aufzählung ist nicht abschließend („insbesondere“), DSFA daher auch erforderlich z. B. bei systematischer Arbeitnehmerüberwachung (per Video oder Arbeitsplatzrechner)

Erfordert BIM eine Datenschutz-Folgenabschätzung (DSFA)? (2)

- Aufsichtsbehörden haben **Liste der Verarbeitungstätigkeiten** erstellt, für die eine DSFA durchzuführen ist.
- Tipp:
  Gerade bei **Großprojekten** mit vielen beteiligten Unternehmen und Beschäftigten **sollte geprüft werden**, ob die Durchführung einer DSFA erforderlich ist.
- Nach dieser Liste ist eine DSFA erforderlich auch bei **umfangreicher Verarbeitung personenbezogener Daten über das Verhalten von Beschäftigten**, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben oder diese Betroffenen in anderer Weise erheblich beeinträchtigt werden.
- Der **Datenschutzbeauftragte berät** bei der Durchführung der DSFA.
- Art. 35 Abs. 7 gibt **Mindestinhalte** der DSFA vor.

Höhere Bußgelder

- Verstöße gegen organisatorische Regelungen, Art. 83 Abs. 4
  - Geldbußen von bis zu **10.000.000 EUR**
  - im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres
- Verstöße gegen Grundsätze und Betroffenenrechte etc., Art. 83 Abs. 5
  - Geldbußen von bis zu **20.000.000 EUR**
  - im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres
- Höhe der Geldbuße muss im Einzelfall **wirksam, verhältnismäßig und abschreckend** sein, Art. 83 Abs. 1

Rechtsschutz der betroffenen Personen

- **Beschwerde bei der Aufsichtsbehörde**, Art. 77
  Beschwerderecht für Betroffene **bei „einer Aufsichtsbehörde“**, („insbesondere“ am Ort ihres gewöhnlichen Aufenthaltsortes im Mitgliedstaat, ihres Arbeitsplatzes oder des mutmaßlichen Verstoßes)
  - Beschwerdeeingänge beim LfD haben deutlich zugenommen
- **Klagerecht gegen die Aufsichtsbehörde**, Art. 78
  - bisher noch nicht in Anspruch genommen
- **Direktes Klagerecht**, Art. 79
  gegen die für die Verarbeitung Verantwortlichen oder gegen deren Auftragsverarbeiter, Vertretung betroffener Personen durch Verbände möglich, Art. 80 Abs. 1
  - das Risiko besteht, wie einige veröffentlichte Urteile zeigen
- **Verbandsklagerecht** , Art. 80 Abs. 2
  Fortgeltung § 2 Abs. 2 Nr. 11 UKlaG
  - Ziel der Verbände ist derzeit eher, massenhafte Datenschutzverstöße von Großkonzernen zu unterbinden (Facebook, WhatsApp)

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

- **Ethischer und 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)

Fazit

- BIM lässt sich datenschutzkonform betreiben
- Es bedarf der Berücksichtigung des Datenschutzes:
  - bei jeglicher Verarbeitung personenbezogener Daten
  - Vertrag als Rechtsgrundlage
  - dem Risiko angepasste technische und organisatorische Maßnahmen
  - Datenminimierung, Zweckbindung

Weitere Informationen und Beratungen

- Im Unternehmen: Datenschutzbeauftragte
- https://datenschutz.sachsen-anhalt.de/
  insbesondere: Kurzpapiere der DSK zu wesentlichen Themen
- https://www.bfdi.bund.de/DE/Datenschutz/datenschutz-node.html
- Kammern
- Branchenverbände
- https://www.gdd.de/
- https://www.bvdnet.de/
- https://www.datenschutzverein.de/
- https://www.bmi.bund.de/SharedDocs/topthemen/DE/topthema-datenschutz/top-thema-datenschutz.html

Vielen Dank für Ihre Aufmerksamkeit!

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
Telefax: 0391 81803-33