



SACHSEN-ANHALT

Landesbeauftragter
für den Datenschutz

Wesentliche Regelungen der Europäischen Datenschutz-Grundverordnung und des neuen Bundesdatenschutzgesetzes für Vereine

Carsten Nock

Referatsleiter beim Landesbeauftragten
für den Datenschutz

Agenda

- **Grundlegende Aspekte**
- **Gliederung der DS-GVO und Anwendungsbereich**
- **Verbot mit Erlaubnisvorbehalt**
- **Anforderungen an die Verarbeitung personenbez. Daten**
- **Weitere Prinzipien, Betroffenenrechte**
- **Dokumentations- und Nachweispflichten**
- **Datenschutz-Folgenabschätzung**
- **Meldepflicht**
- **Der betriebliche Datenschutzbeauftragte**
- **Technischer Datenschutz**
- **Beschäftigtendatenschutz**
- **Bußgelder, Rechtsschutzmöglichkeiten der Betroffenen**



Ausgangslage (1)

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



Ausgangslage (2)

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)“



Ziele der DS-GVO

- Harmonisierung, gleichmäßig hohes Datenschutzniveau
 - ein **einheitliches Datenschutzrecht** in der EU (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)



Anwendung der DS-GVO

- Seit dem 25. Mai **2016**: DS-GVO **in Kraft**
- Seit dem 25. Mai **2018**: DS-GVO **anzuwenden**
 - Artikel 99: in **allen Teilen verbindlich** und **unmittelbare Geltung** in **jedem** Mitgliedstaat (anders als Richtlinie von 1995)



Geltung der DS-GVO

- Viele **Regelungsspielräume** zugunsten der Mitgliedstaaten
 - teilweise zwingend umzusetzen (z. B. zu Zertifizierungen, Art. 42, 43)
 - oder nur Optionen (z. B. kann das Alter für die Einwilligungsfähigkeit von 16 auf bis zu 13 Jahre herabgesetzt werden, im **BDSG-neu** aber nicht umgesetzt)
- Regelungsspielräume beschränken die Harmonisierung (**Grund-Verordnung**)!



Weitere Regelungen zur Umsetzung der 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>)
- **Bundesebene**
„Datenschutz-Anpassungs- und Umsetzungsgesetz EU - DSAnpUG-EU“ (BGBl. I Nr. 44 v. 5.7.2017, S. 2097);
darin enthalten: **BDSG-neu**, Anpassung von zahlreichen **spezialgesetzlichen Regelungen**
- **Länderebene**
 - Entwicklung neuer **Landesdatenschutzgesetze**
 - Anpassung von zahlreichen **spezialgesetzlichen Regelungen**



Umsetzung in Sachsen-Anhalt

- **Neufassung des allgemeinen Datenschutzrechts :**
 1. Regelungen zur **Organisationsfortentwicklung** des Landesbeauftragten für den Datenschutz (LfD)
darin: Konkretisierung der „**völligen Unabhängigkeit**“, z. B. eigener Einzelplan und Personalhoheit, LfD bleibt Teil der unmittelbaren Landesverwaltung; LfD erhält **Anordnungsbefugnis** gegenüber Behörden, in Kraft getreten am 06.05.2018
 2. **Materielle** Regelungen innerhalb des DSG LSA
Gesetz zur Ausfüllung der DS-GVO (DSAG LSA, Ende 2018)
bis dahin: DSG-LSA i. d. F. vom 6. Mai 2018
 3. Gesetz zur Umsetzung der **Jl-Richtlinie** (DSUG LSA, Herbst 2018)
- Anpassung **Fachgesetze** des **bereichsspezifischen Datenschutzes** durch die zuständigen Ressorts (auch SOG LSA)



Konkretisierung der DS-GVO

- **Delegierte Rechtsakte**

Befugnis der **EU-Kommission**, Rechtsakte mit allgemeiner Geltung zu erlassen (z. B. Festlegung von Anforderungen zu datenschutzspezifischen Zertifizierungen, Art. 43 Abs. 8)

- **Durchführungsrechtsakte**

Befugnis der **EU-Kommission**, die Durchführung der DS-GVO durch Rechtsakte zu regeln (eigentlich Sache der Mitgliedstaaten; z. B. Festlegung von technischen Standards für Zertifizierungsverfahren, Art. 43 Abs. 9)

- **Leitlinien, Empfehlungen und bewährte Verfahren**

durch den **Europäischen Datenschutzausschuss**, Art. 70



Gliederung der DS-GVO (1)

- Text beginnt mit **173 Erwägungsgründen** (EG'e)
diese enthalten vereinzelt verbindliche Regelungen, dienen
aber insbesondere der **Auslegung** der folgenden Artikel

Es folgen **99 Artikel** mit umfangreichen Regelungen

Bsp.: **Art. 6 Abs. 1f** gestattet die Verarbeitung personenbezogener Daten, wenn ein berechtigtes Interesse vorliegt. **EG 47** erläutert das berechnigte Interesse. Die Direktwerbung (auch Spendenwerbung) kann ein berechtigtes Interesse sein.



Gliederung der DS-GVO (2)

Kapitel I:	Allgemeine Bestimmungen
Kapitel II:	Grundsätze
Kapitel III:	Rechte der betroffenen Person
Kapitel IV:	Verantwortlicher und Auftragsverarbeiter
Kapitel V:	Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen
Kapitel VI:	Unabhängige Aufsichtsbehörden
Kapitel VII:	Zusammenarbeit und Kohärenz
Kapitel VIII:	Rechtsbehelfe, Haftung und Sanktionen
Kapitel IX:	Vorschriften für besondere Verarbeitungssituationen
Kapitel X:	Delegierte Rechtsakte und Durchführungsrechtsakte
Kapitel XI:	Schlussbestimmungen



Sachlicher Anwendungsbereich, Art. 2

- Die DS-GVO und das BDSG-neu gelten für die:
 - **ganz/teilweise automatisierte** Verarbeitung **personenbezogener Daten**
 - **nichtautomatisierte** Verarbeitung personenbezogener Daten, die in einem **Dateisystem** gespeichert sind oder gespeichert werden sollen (inkl. Akten, soweit sie nach bestimmten Kriterien geordnet sind; vgl. EG 15, Art. 4 Nr. 6), **§ 1 Abs. 1 BDSG-neu**, beim **Beschäftigtendatenschutz** ist § 26 BDSG-neu auch anzuwenden, wenn Daten nicht in einem Dateisystem gespeichert werden
- Keine Geltung bei Datenverarbeitungen, die
 - vom **EU-Recht ausgenommen** sind (z. B. Nachrichtendienste)
 - unter die gemeinsame **Außen- und Sicherheitspolitik** fallen
 - ausschließlich **persönliche / familiäre Tätigkeit** von natürlichen Personen sind
 - unter die **JI-Richtlinie** fallen (Strafverfolgung, polizeiliche Gefahrenabwehr)
 - die Bereitstellung öffentlicher elektronischer **Kommunikationsdienste** in öffentlichen Netzen betreffen, Art. 95 (hier soll demnächst gelten die Verordnung über Privatsphäre und elektronische Kommunikation)



Verbot mit Erlaubnisvorbehalt (1)

EU-Grundrechtecharta, Art. 8 Abs. 2:

Personenbezogene 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“.

Daraus folgt: weiterhin **Verbot mit Erlaubnisvorbehalt**

- Art. 6 Abs. 1 DS-GVO: Verarbeitung ist nur rechtmäßig, wenn eine **Einwilligung** vorliegt oder eine andere in der **Vorschrift** genannte Fallgruppe erfüllt ist. Ansonsten ist sie verboten!
- Hier **kein risikobasierter** Ansatz!
- Einfache und komplexe Datenverarbeitungen werden hier gleich behandelt.



Verbot mit Erlaubnisvorbehalt (2)

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

- **Einwilligung**
- **Vertrag (dazu zählt auch die Vereinsmitgliedschaft)**
- **Rechtliche Verpflichtung**
- Lebenswichtige Interessen
- Öffentliches Interesse/hoheitliche Aufgaben
- **Interessenabwägung:** berechtigtes Interesse ./.. schutzwürdiges Interesse (unter besonderer Berücksichtigung der Rechte des Kindes, „Kind“ meint hier alle Minderjährigen) - gilt nicht für Behörden in Erfüllung ihrer Aufgaben



Einwilligung, Art. 7, EG 32, 33, 42, 43

Freiwilligkeit

- Einwilligung ist „**keine gültige Rechtsgrundlage**“ für die Verarbeitung, wenn „**ein klares Ungleichgewicht besteht**“ und es deshalb unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben werden würde (EG 43) – dies kann z. B. im Verhältnis zu Beschäftigten des Vereins vorliegen
- Einwilligung gilt i. d. R. nicht als erteilt, wenn die **Erfüllung eines Vertrages**, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist (**Koppelungsverbot**)



Einwilligung (Fortsetzung)

- Wenn Einwilligung im Zusammenhang mit anderen schriftlichen Erklärungen erfolgt, muss das Ersuchen um Einwilligung in **verständlicher und leicht zugänglicher Form, in klarer und einfacher Sprache erfolgen**, sodass es von anderen Sachverhalten klar zu unterscheiden ist
- Einwilligung ist **jederzeit widerrufbar**, betroffene Person wird vor der Abgabe der Einwilligung hiervon **in Kenntnis gesetzt**
- Form: **formfrei**, muss aber **nachgewiesen** werden
- Einwilligungen von **Kindern** sind nur wirksam, wenn sie in der Lage sind, die **Folgen der Verwendung ihrer Daten einzuschätzen** und sich deshalb verbindlich dazu äußern können
Bei Kindern unter ca. 14 Jahren ist dies regelmäßig zu verneinen. Im **Online-Bereich** können Kinder erst ab **16 Jahren** wirksam einwilligen, Art. 8. Ggf. ist Einwilligung der **Sorgeberechtigten** einzuholen
- Widerruf muss so einfach sein wie die Einwilligung



Datenerhebung von Mitgliedern

Erhoben werden können:

- alle Daten, die zur **Verfolgung des Vereinszwecks** (aus Satzung) und der **Betreuung/Verwaltung** erforderlich sind, Art. 6 Abs. 1 S. 1 b) (Name, Anschrift, oft Geburtsdatum, „Vereinsinteressen“, Schuhgröße??)
- weitere Daten zur **Wahrnehmung berechtigter Interessen**, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten des Mitglieds überwiegen, Art. 6 Abs. 1 S. 1 f) (Familienstand eher nicht, Gesichtsbild erforderlich?) – Vorsicht bei Abwägung! Besonders zu beachten sind Interessen und Rechte der **Kinder** (= alle Minderjährigen)
- weitere Daten aufgrund einer freiwillig erteilten und nachzuweisenden **Einwilligung** (z. B. Lichtbilder?)



Verarbeitungen von Mitgliederdaten

Im Rahmen der Vereinszwecks sind Verarbeitungen zulässig für

- Mitgliederverwaltung
- Mitteilung an Verbände
- Erstellung von Spielerpässen
- Meldungen zu (Sport-)Veranstaltungen

soweit sie erforderlich sind. Fragestellung:

Welche **Einzel**daten des Mitglieds sind wirklich zur Zweckerfüllung erforderlich?



Verarbeitung von Daten Dritter

Ist zulässig

- bei Vertragspartnern, soweit **für die Vertragserfüllung erforderlich**
- bei Besuchern, Gästen, Kursteilnehmern etc. soweit für den jeweiligen („vertragsähnlichen“) Zweck erforderlich
Fragestellung: Werden Daten von Besuchern, Gästen, Kursteilnehmern wirklich benötigt, wenn ja, welche?
- wenn **Interessenabwägung** nach § 6 Abs. 1 S. 1 f) dies zulässt
- wenn wirksame **Einwilligung** vorliegt



Wer darf im Verein personenbezogene Daten nutzen?

Jeder **Funktionsträger** darf nur die für die **Erfüllung seiner Aufgaben** erforderlichen Mitgliederdaten verarbeiten

z. B. reichen oft

- dem mit dem Bankeinzug beauftragten **Kassierer** Name, Anschrift, Bankverbindung ;
- dem **Kursleiter** die Namen der Kursteilnehmer (was ist noch erforderlich?)
- bei weiteren **Funktionsträgern** konkrete **Aufgabe** beachten



Datenübermittlung an Dritte (1)

- Übermittlung an **Mitglieder** ist zulässig, wenn
 - der satzungsgemäße Vereinszweck darin besteht, persönliche oder geschäftliche **Kontakte zu pflegen** (steht das in Satzung?)
 - ein **berechtigtes Interesse** besteht und Interessen oder Grundrechte und Grundfreiheiten der Mitglieder nicht überwiegen (selten)
 - eine wirksame **Einwilligung** vorliegt (**regelmäßig erforderlich**)
- **Aushänge** und **Vereinspublikationen**
 - = i. d. R. Übermittlung an einen unbestimmten Personenkreis,
 - Frage: ist diese Übermittlung **für den Vereinszweck erforderlich** bzw. fällt Interessenabwägung zugunsten des Vereins aus? Letzteres kann bei Funktionsträgern/Ansprechpartnern, Mannschaftsaufstellungen oder Spielergebnissen der Fall sein
 - persönliche Informationen (Eintritte, Austritte, Spenden, Jubiläen, Geburtstagslisten) nur, wenn **Interessen des Mitglieds nicht überwiegen** (Letzteres wird oft der Fall sein)
 - **Einwilligung** (z. B. erforderlich für zu veröffentlichende Mitgliederlisten)



Datenübermittlung an Dritte (2)

- **An Dachverbände und Vereine** zulässig
 - zur **Verwirklichung der Vereinsziele** (Durchführung von gemeinsamen Veranstaltungen) bzw. wenn Interessen des Mitglieds nicht überwiegen
 - an **Dachverbände**, wenn Verpflichtung des Vereins besteht und Übermittlung der Vereinssatzung zu entnehmen ist bzw. Interessen des Mitglieds nicht überwiegen
- **Sponsoren und zu Werbezwecken**
sind regelmäßig nicht vom Vereinszweck gedeckt
- **Versicherungen**
im Rahmen eines Gruppenversicherungsvertrages nur zulässig, wenn **Einwilligung** vorliegt
- **Gemeinden** oder andere **finanzierende Behörden**
können aufgrund einer rechtlichen Verpflichtung zulässig sein (Art. 6 Abs. 1 S. 1 c)) oder wenn Interessensabwägung zugunsten Übermittlung ausfällt



Veröffentlichungen im Internet

Risiken: weltweite Abrufbarkeit, elektronische Recherchierbarkeit, Veränderbarkeit, unbefugte Nutzung

- **Grundsätzlich**

ist die Veröffentlichung personenbezogener Daten durch einen Verein im Internet **unzulässig**, wenn die betroffenen Personen nicht in Kenntnis der Umstände der Veröffentlichung und des Risikos **eingewilligt** haben

- **Ausnahmen**

- „dienstliche“ Kontaktdaten von **Funktionsträgern**
- kurzzeitige Einstellung von Spielergebnissen, Mannschaftsaufstellungen, Veranstaltungsteilnehmern, wenn keine schutzwürdigen Interessen überwiegen
- Einwilligung



Veröffentlichung von Fotografien

- **Portraitfotos** u. ä. (Einzelperson(en) sind prägend für das Foto) in aller Regel **Einwilligung** erforderlich
- **Fotos von Veranstaltungen**
Anfertigung und Veröffentlichung ist zulässig zur **Wahrung berechtigter Interessen** des Vereins, sofern nicht die **Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen** (Art. 6 Abs. 1 S. 1 f).

Bei der Veröffentlichung zu **journalistischen Zwecken** (eigene Bearbeitung in Beziehung auf meinungsbildende Wirkung muss prägend sein) ist **§ 23 KUG** heranzuziehen (OLG Köln v. 18.06.2018, 15 W 27/18) mit ähnlichen Wertungen.



Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie

§ 23

(1) Ohne die nach § 22 erforderliche Einwilligung dürfen verbreitet und zur Schau gestellt werden:

1. Bildnisse aus dem Bereiche der **Zeitgeschichte**;
2. Bilder, auf denen die Personen nur als **Beiwerk** neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;
3. Bilder von **Versammlungen, Aufzügen und ähnlichen Vorgängen**, an denen die dargestellten Personen teilgenommen haben;
4. ...

(2) Die Befugnis erstreckt sich jedoch nicht auf eine Verbreitung und Schaustellung, durch die ein **berechtigtes Interesse** des Abgebildeten oder, falls dieser verstorben ist, seiner Angehörigen **verletzt wird**.

Empfehlung: bei Veranstaltungen auf Veröffentlichung von Fotos hinweisen.



Textvorschlag für eine Einwilligungserklärung zur Veröffentlichung im Internet

„...Der Vereinbeabsichtigt zur Vorstellung seiner Arbeitsgruppen in der Öffentlichkeit Fotografien anzufertigen und im Internet auf seiner Homepage für die Dauer eines Jahres zu veröffentlichen, auf denen die Mitglieder erkennbar sein sollen.

Wir weisen darauf hin, dass die Fotos bei der Veröffentlichung im Internet weltweit abrufbar sind. Eine Weiterverwendung oder Veränderung dieser Fotos durch Dritte kann daher nicht generell ausgeschlossen werden.

Zur Veröffentlichung im Internet wird die Einwilligung der abgelichteten Mitglieder benötigt. Die Einwilligung ist jederzeit widerrufbar. Durch den Widerruf wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt....

Ich habe den obigen Text zur Kenntnis genommen und willige freiwillig in die Veröffentlichung eines Fotos von mir für ein Jahr auf der Homepage des Vereins ein.

...Name, Datum, Ort und Unterschrift des Mitglieds...“



Weitere 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-, Lösungsrechte
- **Datensicherheit**
- **Unabhängige Datenschutzaufsicht** mit Abhilfebefugnissen, jetzt auch gegenüber Behörden, inkl. Kommunen



Betroffenenrechte - Überblick (1)

- **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**
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 Einschränkung der Verarbeitung, Art. 18**



Betroffenenrechte - Überblick (2)

- **Neues 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
[Arbeitspapier der Art.-29-Gruppe unter http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083)
- **Widerspruchsrecht, Art. 21**
Recht besteht in besonderen Situationen (z. B. Gefahr für Leib oder Vermögen) bei Datenverarbeitungen, die auf Interessensabwägung beruhen (auch Profiling); Folge des Widerspruchs: keine Weiterverarbeitung,
Ausnahme: zwingende Gründe o. Rechtsverteidigung



Beschränkung der Betroffenenrechte, Art. 23

...ist möglich aufgrund **mitgliedstaatlicher Rechtsvorschriften**, sofern **Wesensgehalt** der Grundrechte und Grundfreiheiten geachtet wird und sie eine notwendige und **verhältnismäßige Maßnahme** darstellt, die unter anderem Folgendes sicherstellt:

- a) nationale Sicherheit
- c) öffentliche Sicherheit
- d) Strafverfolgung
- e) wichtige Ziele allgemeinen öffentlichen Interesses
- i) Rechte und Freiheiten anderer Personen
- j) Durchsetzung zivilrechtlicher Ansprüche

Jetzt in **§§ 32 – 37 BDSG-neu** geregelt



Informationspflichten bei der Erhebung bei betroffener Person, Art. 12, 13, EG 58 ff

- **Neue Informationsinhalte:** z. B. Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten, Rechtsgrundlage der Datenverarbeitung, Interessenabwägung, Drittstaatentransfer, Dauer der Speicherung oder Kriterien der Festlegung der Dauer, bestimmte Betroffenenrechte, Recht auf Widerruf der Einwilligung, automatisierte Entscheidungsfindung einschließlich Profiling; Art. 13 Abs. 1 u. 2
 - Information muss **auch** erfolgen, wenn Daten aus **öffentlichen Quellen** stammen
 - Zeitpunkt: bei Erhebung
 - **Form:** schriftlich, elektronisch, mündlich (wenn Identität nachgewiesen)
 - Pflicht **entfällt**
 - wenn Betroffener über Information verfügt, Art. 13 Abs. 3
 - bei Weiterverarbeitung
 - analog gespeicherter Daten, wenn Interesse der betroffenen Person gering ist
 - Information würde öffentliche Sicherheit, Ordnung, Rechtsverteidigung oder vertrauliche Übermittlung an öffentliche Stellen gefährden, **§ 32 Abs. 1 BDSG-neu**
- Entfällt die Pflicht, sind gemäß **§ 32 Abs. 2 BDSG-neu** **Schutzmaßnahmen** zu treffen (z. B. öffentliche Information) und ist der Grund zu dokumentieren



Hinweise auf die Rechte der Betroffenen

Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf **Auskunft** über diese personenbezogenen Daten und auf die in Art. 15 DSGVO im einzelnen aufgeführten Informationen.

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die **Berichtigung** sie betreffender unrichtiger personenbezogener Daten und ggf. die Vervollständigung unvollständiger personenbezogener Daten zu verlangen (Art. 16 DSGVO).

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der in Art. 17 DSGVO im einzelnen aufgeführten Gründe zutrifft, z. B. wenn die Daten für die verfolgten Zwecke nicht mehr benötigt werden (Recht auf **Löschung**).

Die betroffene Person hat das Recht, von dem Verantwortlichen die **Einschränkung der Verarbeitung** zu verlangen, wenn eine der in Art. 18 DSGVO aufgeführten Voraussetzungen gegeben ist, z. B. wenn die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat, für die Dauer der Prüfung durch den Verantwortlichen.

Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten **Widerspruch** einzulegen. Der Verantwortliche verarbeitet die personenbezogenen Daten dann nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 21 DSGVO).

Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf **Beschwerde bei einer Aufsichtsbehörde**, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt (Art. 77 DSGVO). Die betroffene Person kann dieses Recht bei einer Aufsichtsbehörde in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes geltend machen. In Sachsen-Anhalt ist die zuständige Aufsichtsbehörde der Landesbeauftragte für den Datenschutz, Leiterstraße 9, 39104 Magdeburg.



Informationspflichten bei Dritterhebung, Art. 12, 14, EG 58 ff

- **Neue Informationsinhalte:** ähnlich Art. 13 Abs. 1 u. 2, zusätzlich: zu verarbeitende Datenkategorien und Datenquelle
- Zeitpunkt: spätestens nach einem Monat, Art. 14 Abs. 3
- Form: wie bei Art. 13
- Pflicht entfällt z. B. wenn:
 - Betroffener über Information verfügt, bei unverhältnismäßigem Aufwand, Berufsgeheimnis (Art. 14 Abs. 3)
 - durch Information Rechtsverteidigung (§ 33 Abs. 1 Nr. 2a BDSG-neu) oder
 - öffentliche Sicherheit oder Ordnung gefährdet wäre - hier Feststellung einer öffentlichen Stelle erforderlich (§ 33 Abs. 1 Nr. 2b BDSG-neu)

Entfällt die Pflicht nach § 33 BDSG-neu, sind **Schutzmaßnahmen** zu treffen (z. B. öffentliche Information) und es ist der Grund zu dokumentieren



Auskunftsrecht, Art. 12, 15

- Beinhaltet die Pflicht, **auf Verlangen** die in Art. 15 Abs. 1 genannten Informationen zu erteilen (ähnlich Art. 13 u. 14)
- Frist:
unverzüglich, spätestens innerhalb eines Monats, Art. 12 Abs. 3
- Form
schriftlich, elektronisch (Kopie), auch über sicheren Fernzugriff
- Auskunft entfällt gemäß **§ 34 Abs. 1 BDSG-neu**, wenn
 - Voraussetzungen des **§ 33 Abs 1 Nr. 2b BDSG-neu vorliegen**, oder
 - Daten aufgrund Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder sie nur der Datensicherheit / Datenschutzkontrolle dienen, und Auskunft **unverhältnismäßigen Aufwand** erfordern würde und Verarbeitung zu anderen Zwecken ausgeschlossen ist
- Auskunftsverweigerung nach **§ 34 Abs. 1 BDSG-neu** ist zu **dokumentieren** und regelmäßig zu **begründen**, **§ 34 Abs. 2 BDSG-neu**



Recht auf Löschung, Art. 17

- Pflicht entfällt nach **Art. 17 Abs. 3** , wenn Verarbeitung erforderlich ist
 - zur Ausübung von Meinungsäußerungsfreiheit und Information
 - zur **Erfüllung einer rechtlichen Verpflichtung** (z. B. Steuerrecht)
 - aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit
 - für Archiv-, historische oder statistische Zwecke
 - zur **Rechtsverteidigung**

nach **§ 35 Abs. 1 BDSG-neu**

- im Falle nicht automatisierter Datenverarbeitung, wenn **Aufwand unverhältnismäßig hoch** und Interesse der betroffenen Person gering ist
- wenn Interessen der betroffenen Person entgegenstehen

Wenn Daten aufgrund von § 35 Abs. 1 BDSG-neu nicht gelöscht werden können, dürfen sie nur eingeschränkt verarbeitet werden



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

- kein Verzeichnis erforderlich bei Unternehmen oder Einrichtungen, 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	
Angaben zum Vertreter des Verantwortlichen Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc. Name Straße Postleitzahl Ort Telefon E-Mail-Adresse	
Angaben zur Person des Datenschutzbeauftragten * (extern mit Anschrift) * sofern gem. Artikel 37 DS-GVO benannt Anrede Titel Name, Vorname Straße Postleitzahl Ort Telefon E-Mail-Adresse	



Verarbeitungstätigkeit:		lfd. Nr.:
Benennung: _____		_____
Datum der Einführung:	Datum der letzten Änderung:	
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse (Art. 30 Abs. 1 S. 2 lit a)		
Zwecke der Verarbeitung (Art. 30 Abs. 1 S. 2 lit b)		
Optional: Name des eingesetzten Verfahrens		
Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c)	<input type="checkbox"/> Beschäftigte <input type="checkbox"/> Interessenten <input type="checkbox"/> Lieferanten <input type="checkbox"/> Kunden <input type="checkbox"/> Patienten <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
Beschreibung der Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 S. 2 lit. c)	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Besondere Kategorien personenbezogener Daten (Art. 9): <input type="checkbox"/>	



Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden (Art. 30 Abs. 1 S. 2 lit. d)	<input type="checkbox"/> intern (Zugriffsberechtigte) Abteilung/ Funktion
	<input type="checkbox"/> extern Empfängerkategorie
	<input type="checkbox"/> Drittland oder internationale Organisation (Kategorie)
ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (Art. 30 Abs. 1 S. 2 lit. e)	<input type="checkbox"/> Datenübermittlung findet nicht statt und ist auch nicht geplant <input type="checkbox"/> Datenübermittlung findet wie folgt statt:
Nennung der konkreten Datenempfänger	<input type="checkbox"/> Drittland oder internationale Organisation (Name)
Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	Dokumentation geeigneter Garantien
Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 S. 2 lit. f)	

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 DSGVO (Art. 30 Abs. 1 S. 2 lit. g)
Siehe TOM-Beschreibung in den „Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten“, Ziff. 6.7. und 6.8

.....
 Verantwortlicher

.....
 Datum

.....
 Unterschrift



SACHSEN-ANHALT

Landesbeauftragter
 für den Datenschutz

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
- **Einwilligung**, Art. 7 Abs. 1 (kein zwingendes Schriftformerfordernis, muss aber nachgewiesen werden)
- **Datenschutz-Organisation**, Art. 24 Abs. 1, einschließlich technischer Maßnahmen, Art. 25 und 32
- 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. – Vorsicht bei Cloudprodukten: Wo steht der Datenspeicher?



Datenschutz-Folgenabschätzung (DSFA), Art. 35

Es handelt sich um eine **risikobezogene Pflicht** des für die Verarbeitung Verantwortlichen

- Durchführung erforderlich, wenn Verarbeitung **voraussichtlich ein hohes Risiko** für die persönlichen Rechte und Freiheiten zur Folge hat, Art. 35 Abs. 1
- Art. 35 Abs. 3 nennt Situationen, die eine DSFA erfordern (Abs. 3 Buchst. c): „**systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche**“, z. B. Überwachung eines gesamten Sportfestes)
- Die Aufzählung ist nicht abschließend, LfD führt Liste für DSFA-Vorgänge unter <https://datenschutz.sachsen-anhalt.de/informationen/internationales/datenschutz-grundverordnung/liste-von-verarbeitungstaetigkeiten-mit-erforderlicher-datenschutz-folgenabschaetzung/>
- Art. 35 Abs. 7 gibt Mindestinhalte der DSFA vor (ähnlich wie bisherige Vorabkontrolle)



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**)
- 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.“
Bsp: 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 auf der Homepage des LfD



Ein Datenschutzbeauftragter ist zu benennen:

- nach **§ 38 BDSG 2018**
 - soweit in der Regel mindestens **zehn Personen (es zählen auch Ehrenamtliche)** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind oder
 - wenn Verantwortliche oder Auftragsverarbeiter einer **Datenschutz-Folgenabschätzung** (DSFA) nach Art. 35 DS-GVO unterliegen;
 - wenn Verarbeitung zur geschäftsmäßigen Übermittlung, Markt- und Meinungsforschung erfolgt
- nach **Art. 37 DS-GVO wenn**
 - Kerntätigkeit aus Verarbeitungen besteht, die umfangreiche regelmäßige und systematische Überwachung erfordern
 - Kerntätigkeit in der **umfangreichen Verarbeitung besonderer Kategorien** nach Art. 9 DS-GVO besteht (inkl. Gesundheitsdaten)



Stellung des DSB, Art. 38

Der DSB

- ist frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen **eingebunden**
- ist durch Ressourcen und Zugang zu Verarbeitungsvorgängen **zu unterstützen**
- ist **weisungsfrei**, darf wegen der Erfüllung seiner Aufgabe nicht abberufen oder benachteiligt werden, berichtet unmittelbar der Führungsebene
- kann von betroffenen Personen **zu Rate gezogen** werden
- ist an **Geheimhaltung und Vertraulichkeit** gebunden
- kann **andere Aufgaben** wahrnehmen, sofern **kein Interessenkonflikt** vorliegt (nicht: IT-Leiter)
- kann nach **§§ 38 Abs. 2, 6 Abs. 4 BGSG-neu** nur bei Vorliegen eines **wichtigen Grundes** i. S. v. § 626 BGB **abberufen und gekündigt** werden



Aufgaben des DSB, Art. 39

- **Unterrichtung und Beratung** der Verantwortlichen, Auftragsverarbeiter und Beschäftigten
- **Überwachung** der Einhaltung der Datenschutzvorschriften (bDSB führt die Datenverarbeitung nicht durch!)
- Beratung im Zusammenhang mit der **Datenschutz-Folgenabschätzung**
- **Zusammenarbeit** mit der **Aufsichtsbehörde**
- **Anlaufstelle** für Aufsichtsbehörde
- Es entfällt: Verfügbarmachen des Verfahrensverzeichnis für Jedermann

- **Aufgabe des Verantwortlichen und des Auftragsverarbeiters**
Veröffentlichung der Kontaktdaten des DSB und Mitteilung an die Aufsichtsbehörde, Art. 37 Abs. 7
Onlineformular auf der Homepage des LfD



Wer kann zum DSB bestellt werden, Art. 37 Abs. 5, 6

- Der DSB wird aufgrund seiner **beruflichen Qualifikation** und insbesondere seines **Fachwissens** auf dem Gebiet des
 - **Datenschutzrechts (DS-GVO, BDSG-neu, Fachrecht)** und der
 - **Datenschutzpraxis** (erfordert Kenntnisse der **betrieblichen Datenverarbeitung**)
 - sowie seiner Fähigkeiten, die **Aufgaben gemäß Artikel 39 zu erfüllen** (erfordert z. B. **Kommunikationsfähigkeit** – bDSB muss mit Geschäftsleitung, Mitarbeitern und Externen reden können), benannt.
- Der DSB kann als
 - Beschäftigter („**interner**“) oder
 - im Rahmen eines Dienstleistungsvertrages („**externer**“) tätig werden.



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



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

Unter Berücksichtigung

- des **Standes 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, Bsp.: **Verschlüsselung von Onlineformularen mit aktuellem Verschlüsselungsprotokoll**
- 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 (z. B. **SDM**).



Auftragsverarbeitung, Art. 28

- **Fälle:** z. B. Gehaltsabrechnung, Cloud-Computing, IT-Wartung, Werbeadressenverarbeitung durch Lettershop, Datenträgerentsorgung; nicht: Steuerberatung, Rechtsvertretung
- **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
- Vertragsmuster auf der Homepage des LfD
- Bei Pflichtverletzung **haftet** jetzt auch der **Auftragsverarbeiter für Schadensersatz**, Art. 82 Abs. 1, 2, 4



Beschäftigtendatenschutz (1) - Verarbeitung aufgrund Gesetz, Art. 88, § 26 BDSG-neu

- Personenbezogene Daten von Beschäftigten dürfen für **Zwecke des Beschäftigtenverhältnisses** verarbeitet werden, wenn dies **erforderlich** ist:
 - für die **Begründung, Durchführung oder Beendigung des Beschäftigtenverhältnisses**
 - auch auf der Grundlage von **Kollektivvereinbarungen** (einschließlich besonderer Kategorien personenbezogener Daten)
- Zur Ausübung oder Erfüllung der sich aus einem **Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung** (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten
- Zur **Aufdeckung von Straftaten**, wenn zu dokumentierende tatsächliche Anhaltspunkte auf eine Straftat des Beschäftigten vorliegen, die Verarbeitung zur Aufklärung erforderlich ist und keine schutzwürdigen Interessen überwiegen
- § 26 BDSG-neu gilt auch, wenn Daten nicht in einem Dateisystem gespeichert werden, **§ 26 Abs. 7 BDSG-neu** (wie bisher § 32 BDSG)

Die Grundsätze der Datenverarbeitung aus Art. 5 sind einzuhalten.



Beschäftigtendatenschutz (2) - Einwilligung

Die Verarbeitung personenbezogener Daten von Beschäftigten ist grundsätzlich aufgrund einer Einwilligung möglich, soweit sie freiwillig erfolgt. Dies ist nicht gegeben, wenn infolge von Abhängigkeit ein **klares Ungleichgewicht** besteht und es deshalb in Anbetracht aller Umstände unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben werden würde, EG 43.

Voraussetzungen nach **§ 26 Abs. 2 BDSG-neu**:

- **Freiwilligkeit** kann insbes. vorliegen,
 - wenn für die beschäftigte Person ein rechtlicher und wirtschaftlicher **Vorteil** erreicht wird, oder
 - Arbeitgeber und Beschäftigte gleichgelagerte Interessen verfolgen, oder
 - dem Beschäftigten nachteilsfreie Alternativen zur Verfügung stehen
- **Schriftform** ist erforderlich, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist (Nachweispflicht beachten!)
- **Aufklärung** des Beschäftigten in Textform über den **Zweck** der Datenverarbeitung und das Recht, die Einwilligung jederzeit zu widerrufen (Art. 7 Abs. 3).



Videoüberwachung (VÜ) - allgemein

- VÜ kann für Vereine zulässig sein, soweit
 1. sie zur **Wahrung der berechtigten Interessen** (z. B. Hausrecht, Sicherung von Beweismaterial) des Verantwortlichen oder eines Dritten **erforderlich** ist, sofern nicht die **Interessen oder Grundrechte und Grundfreiheiten** der betroffenen Person überwiegen, insbesondere dann, wenn es sich um ein **Kind** handelt (Art. 6 Abs. 1 S. 1 f DS-GVO)
 2. eine wirksame **Einwilligung aller Betroffenen** vorliegt (das Betreten des gekennzeichneten Erfassungsbereichs der Kameras ist keine Einwilligung)
 3. bei Kameras mit **Gesichtserkennung** die engen Ausnahmefällen des **Art. 9 Abs. 2** vorliegen
- Beachte:
 - strenger Maßstab in **Arbeitsverhältnissen**
 - keine VÜ in **Sanitär- oder Saunabereichen**
- **Löschung**: wenn Aufnahmen zur Zweckerreichung nicht mehr notwendig sind (zu Zwecken der Sicherung von Beweismaterial regelmäßig nach **48 Stunden**)
- Bei **Beschaffung** Data Protection by Design beachten



Videüberwachung – Informationspflicht (1)

Beispiel für ein vorgelagertes Hinweisschild nach Art. 13 der Datenschutz-Grundverordnung bei Videoüberwachung¹



Weitere Informationen erhalten Sie:

- per Aushang (wo genau?)
- an unserer Kundeninformation /
Rezeption / Kasse im Erdgeschoss
- (ggf.) zusätzlich im Internet unter ...

Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters:

Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden):

Zwecke und Rechtsgrundlage der Datenverarbeitung:

berechtigte Interessen, die verfolgt werden:

Speicherdauer oder Kriterien für die Festlegung der Dauer:

¹ Hinweis: Die Informationen sind unentgeltlich in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen. Sie können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden (vgl. Art. 12 DSGVO). Um Lesbarkeit zu erreichen, sollte der Ausdruck mindestens in DIN A4 erfolgen.



SACHSEN-ANHALT

Landesbeauftragter
für den Datenschutz

Videüberwachung – Informationspflicht (2)

Beispiel für ein vollständiges Informationsblatt (Aushang) nach Art. 13 der Datenschutz-Grundverordnung bei Videüberwachung¹



Sie finden diese Informationen zusätzlich im Internet unter ...

Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters:
Kontaktadressen des Datenschutzbeauftragten (sofern vorhanden):
Zwecke und Rechtsgrundlage der Datenverarbeitung:
berechtigte Interessen, die verfolgt werden:
Speicherdauer oder Kriterien für die Festlegung der Dauer:
Empfänger oder Kategorien von Empfänger der Daten (sofern Datenübermittlung stattfindet): bei Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln: Informationen über Angemessenheitsbeschluss der Kommission bzw. geeignete oder angemessene Garantien:

Hinweise auf die Rechte der Betroffenen

Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf die in Art. 15 DSGVO im einzelnen aufgeführten Informationen.

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten und ggf. die Vervollständigung unvollständiger personenbezogener Daten zu verlangen (Art. 16 DSGVO).

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der in Art. 17 DSGVO im einzelnen aufgeführten Gründe zutrifft, z. B. wenn die Daten für die verfolgten Zwecke nicht mehr benötigt werden (Recht auf Löschung).

Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der in Art. 18 DSGVO aufgeführten Voraussetzungen gegeben ist, z. B. wenn die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat, für die Dauer der Prüfung durch den Verantwortlichen.

Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten Widerspruch einzulegen. Der Verantwortliche verarbeitet die personenbezogenen Daten dann nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 21 DSGVO).

Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt (Art. 77 DSGVO). Die betroffene Person kann dieses Recht bei einer Aufsichtsbehörde in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes geltend machen. In (Bundesland) ist die zuständige Aufsichtsbehörde: ...

¹ Hinweis: Die Informationen sind unentgeltlich in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen. Sie können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden (vgl. Art. 12 DSGVO). Um Lesbarkeit zu erreichen, sollte der Ausdruck mindestens in DIN A3 erfolgen.



SACHSEN-ANHALT

Landesbeauftragter
für den Datenschutz

Werbung, Spendenaufrufe

- Werbung/Spendenaufrufe sind zulässig, sofern nicht die **Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten** erfordern, die **berechtigten Interessen des Werbenden** überwiegen (Art. 6 Abs. 1f)
Problem: Ist Werbung **absehbar** (EG 47)? Art und Weise, Intensität...
Direktwerbung des Vereins und Spendenaufrufe können zulässig sein.
- Besonderer Schutz für **Kinder** erforderlich, EG 38
„Kind“ nach DS-GVO meint alle nach deutschem Recht **Minderjährigen**
- Beschränkungen des **UWG** sind weiterhin zu beachten
aber: Entwicklung der **Verordnung über Privatsphäre und elektronische Kommunikation beachten**
- Nach **Werbewiderspruch** keine Verarbeitung mehr für Werbung zulässig, Art. 21 Abs. 3



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

- **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)
- **Klagerecht gegen die Aufsichtsbehörde, Art. 78**
- **Direktes Klagerecht, Art. 79**
gegen die für die Verarbeitung Verantwortlichen oder gegen deren Auftragsverarbeiter
- **Vertretung betroffener Personen durch Verbände möglich, Art. 80 Abs. 1**
- **Verbandsklagerecht , Art. 80 Abs. 2**
Fortgeltung § 2 Abs. 2 Nr. 11 UKlaG



Weitere Informationen und Beratungen

- Im Verein: Datenschutzbeauftragte
- <https://datenschutz.sachsen-anhalt.de/datenschutz-sachsen-anhalt/>
insbesondere: **Kurzpapiere der DSK** zu wesentlichen Themen
- <https://www.bfdi.bund.de/DE/Datenschutz/datenschutz-node.html>
- <https://www.gdd.de/>
- <https://www.bvdnet.de/>
- <https://www.datenschutzverein.de/>
- <https://www.youngdata.de/>



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

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



SACHSEN-ANHALT

Landesbeauftragter
für den Datenschutz