
DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO): EIN UPDATE



Dr. Annika Selzer

Leiterin der Forschungsgruppe für Informationsrecht und interdisziplinäre Recht-Technik-Forschung

Hinweis

Die in diesem Vortrag enthaltenen Informationen sind sorgfältig erstellt worden, können eine Rechtsberatung jedoch nicht ersetzen. Eine Haftung oder Garantie dafür, dass die Informationen die Vorgaben der aktuellen Rechtslage erfüllen, wird daher nicht übernommen. Gleiches gilt für die Brauchbarkeit, Vollständigkeit oder Fehlerfreiheit, so dass jede Haftung für Schäden ausgeschlossen wird, die aus der Benutzung dieser Informationen entstehen können. Diese Haftungsbeschränkung gilt nicht in Fällen von Vorsatz.

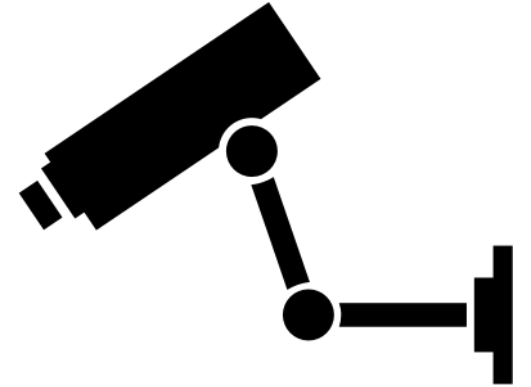
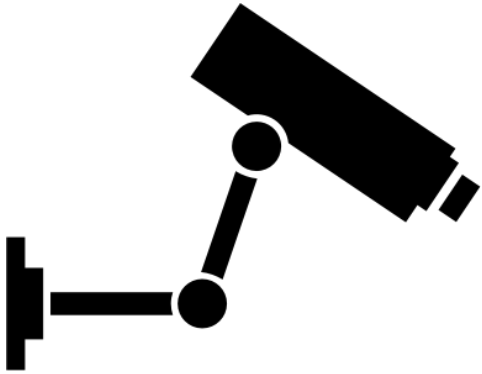
AGENDA

- Warum ist Datenschutz wichtig?
- Was beschäftigt Organisationen seit Anwendbarwerden der DSGVO?
 - Dokumentieren
 - Informieren
 - Löschen

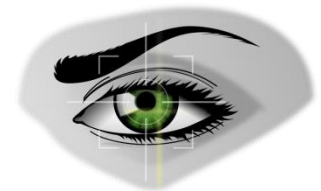
AGENDA

- Warum ist Datenschutz wichtig?
- Was beschäftigt Organisationen seit Anwendbarwerden der DSGVO?
 - Dokumentieren
 - Informieren
 - Löschen

WARUM IST DATENSCHUTZ WICHTIG?



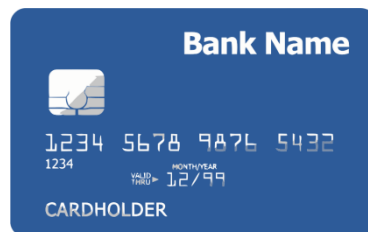
Der Einzelne soll davor bewahrt werden, dass er durch den Umgang mit seinen personenbezogenen Daten in seinen Persönlichkeitsrechten beeinträchtigt wird.



WARUM IST DATENSCHUTZ WICHTIG?

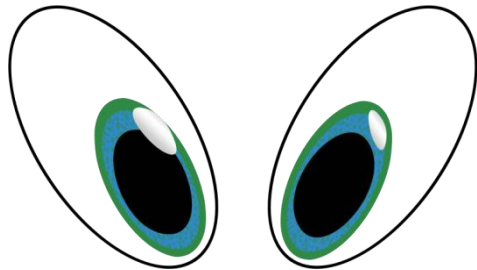
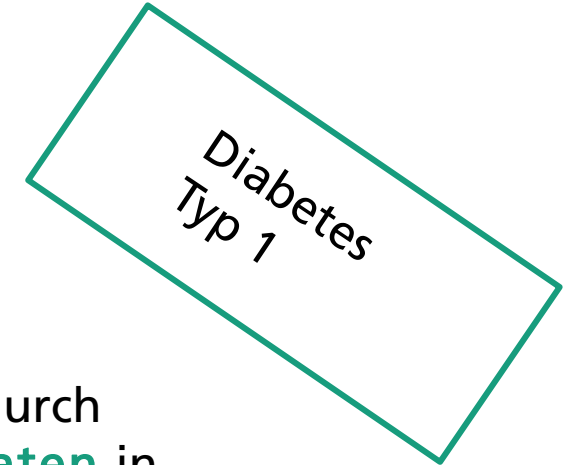


Der Einzelne soll davor bewahrt werden, dass er durch den Umgang mit seinen **personenbezogenen Daten** in seinen Persönlichkeitsrechten beeinträchtigt wird.

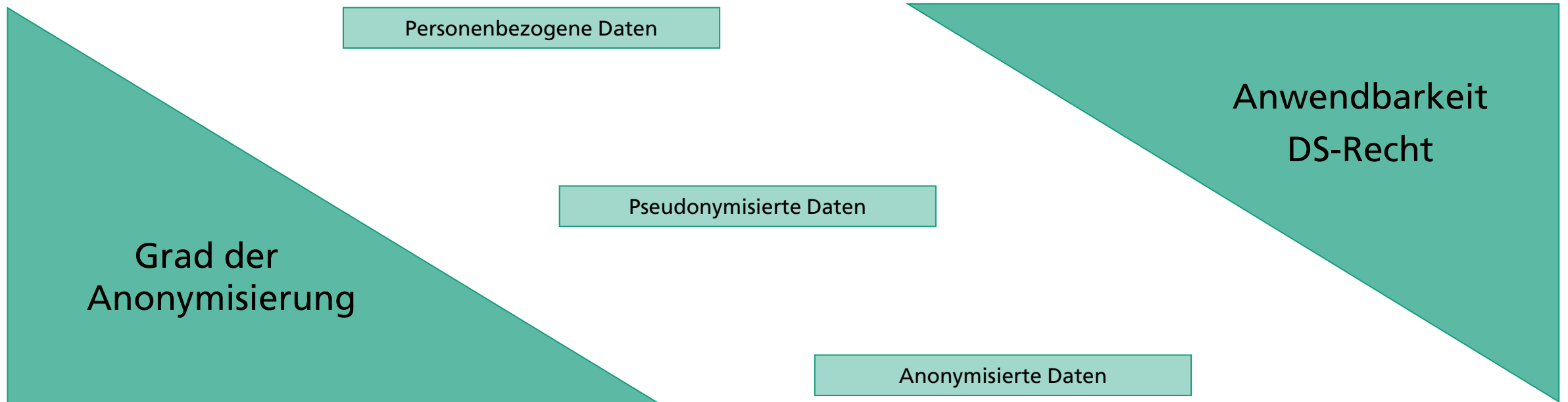


WARUM IST DATENSCHUTZ WICHTIG?

Der Einzelne soll davor bewahrt werden, dass er durch den Umgang mit seinen **personenbezogenen Daten** in seinen Persönlichkeitsrechten beeinträchtigt wird.



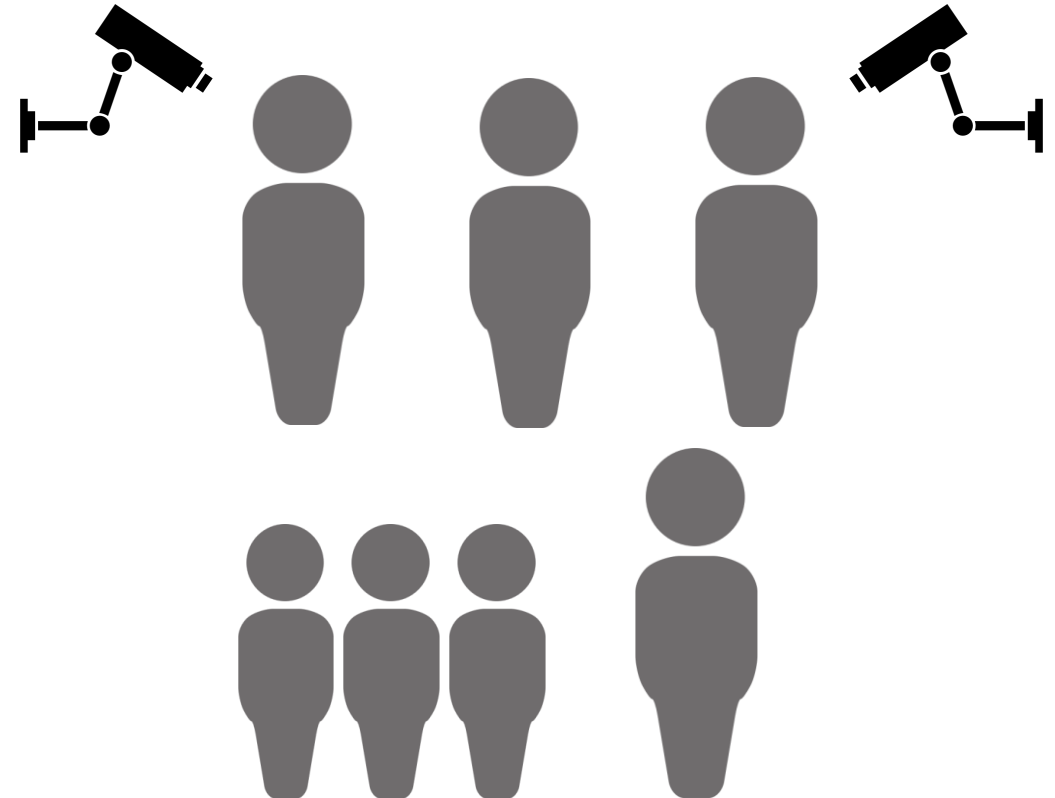
ABGRENZUNG ZWISCHEN PERSONENBEZOGENEN UND ANONYMEN DATEN



UNBEOBACHTET

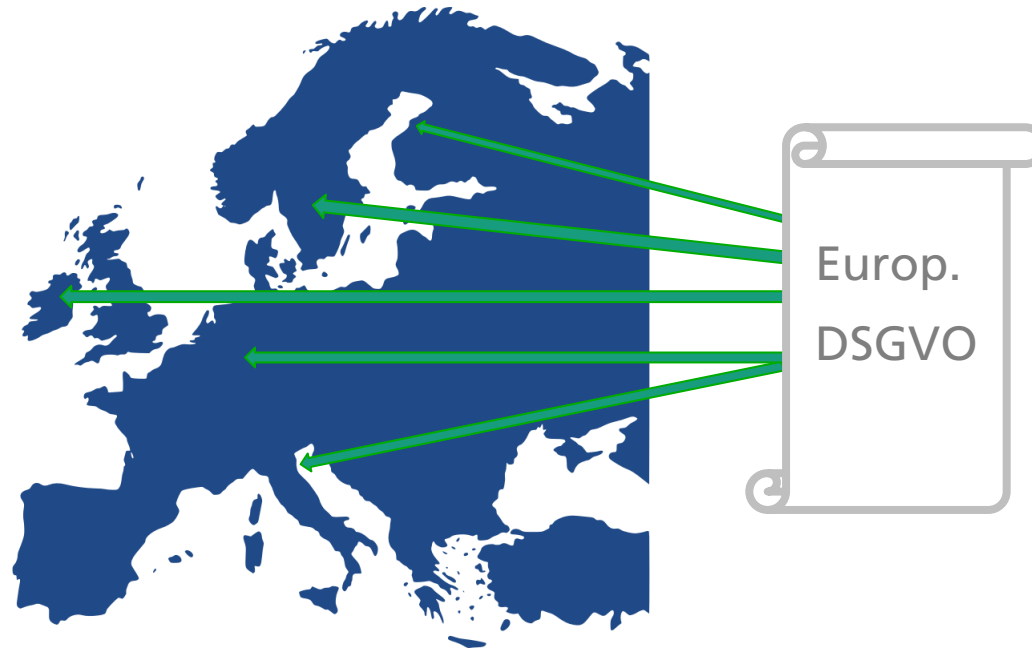
vs.

BEOBACHTET

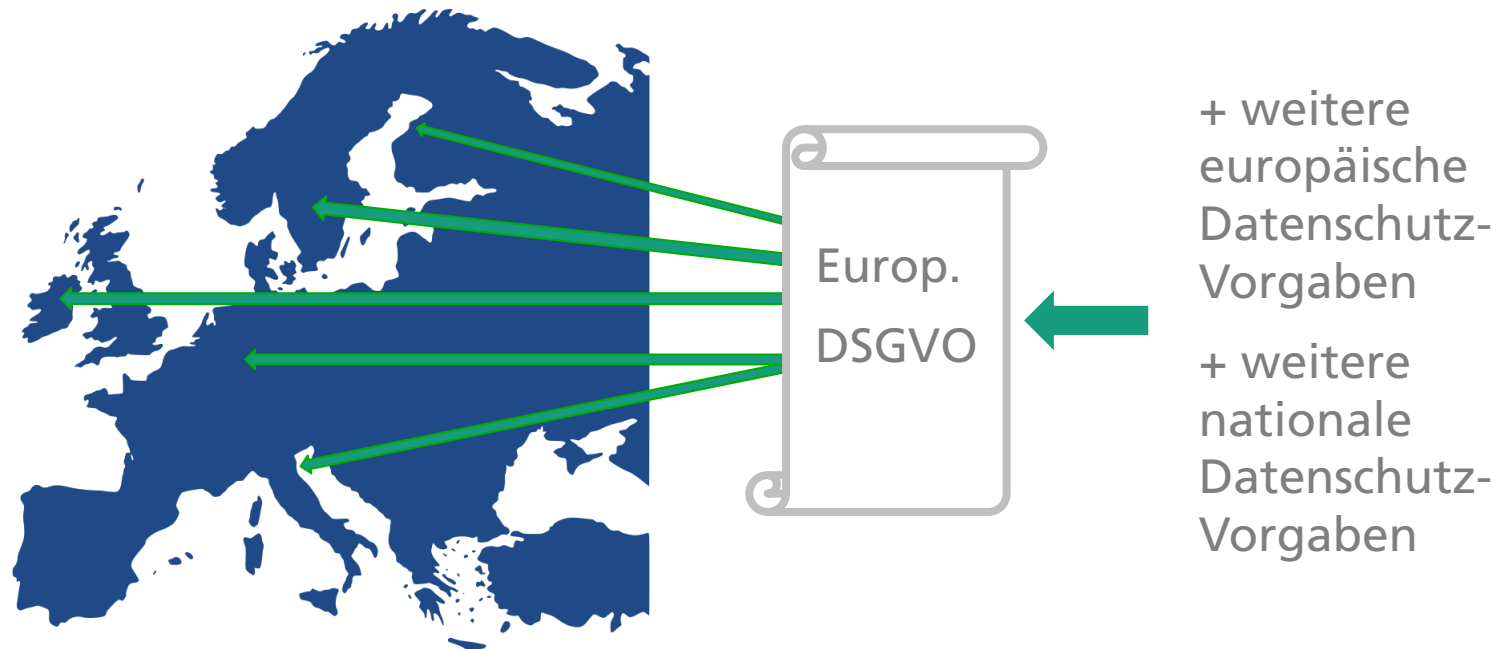


Quelle der Abbildungen: www.openclipart.org (Abruf vor Einstellung des Dienstes)

DATENSCHUTZ IN EUROPA



DATENSCHUTZ IN EUROPA



AGENDA

- Warum ist Datenschutz wichtig?
- Was beschäftigt Organisationen seit Anwendbarwerden der DSGVO?
 - Dokumentieren
 - Informieren
 - Löschen

DAS VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN

- Jeder Verantwortliche muss ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen.
- Das Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.
- Das Verzeichnis ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.
- Die Pflicht zum Führen eines Verzeichnisses der Verarbeitungstätigkeiten gilt nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn
 - die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen,
 - die Verarbeitung erfolgt nicht nur gelegentlich oder
 - es erfolgt eine Verarbeitung besonderer Datenkategorien.

INHALTE DES VERZEICHNISSES (BEI VERANTWORTLICHEN)

- den Namen und die Kontaktdaten des Verantwortlichen die Zwecke der Verarbeitung;
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- die Kategorien von Empfängern;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland sowie die geeigneten Garantien;
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.

INHALTE DES VERZEICHNISSES (BEI AUFTRAGSVERARBEITERN)

- den Namen und die Kontaktdaten des Auftragsverarbeiters und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist;
- die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland sowie die geeigneten Garantien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.

WAS SIND TYPISCHE VERARBEITUNGSTÄTIGKEITEN?

- ...in IT-Abteilungen:
 - Exchange-Server, Telefonsystem, Videoüberwachung.
 - ...
- ...in Marketing-Abteilungen:
 - CRM-System, Webseite, Veranstaltungsmanagement.
 - ...
- ...in der Verwaltung:
 - Reisebuchungsportale, Personalakten, Bewerbungsmanagement.
 - ...
- ...u.V.m., z.B. Projekte mit Probanden, Analysen mit personenbezogenen Echtdaten, Umfragen...

WEITERE FOKUMENTATIONSPFLICHTEN UND -EMPFEHLUNGEN

- Datenschutz- und Löschkonzept (zur Dokumentation über die Ordnungsmäßigkeit der gesamten Verarbeitung) .
- Ggf. Dokumentation der Datenschutz-Folgenabschätzungen .
- Dokumentation/Protokollierung von Einwilligungen, bei
 - schriftlichen Einwilligungen,
 - Einwilligungen auf Webseiten,
 - sonstigen Einwilligungen.
- ...

AGENDA

- Warum ist Datenschutz wichtig?
- Was beschäftigt Organisationen seit Anwendbarwerden der DSGVO?
 - Dokumentieren
 - **Informieren**
 - Löschen

RECHT AUF INFORMATION (ART. 13, 14 DSGVO)

- Die betroffene Person ist sowohl bei Direkterhebung als auch bei Dritterhebung umfangreich über die Datenverarbeitung zu informieren (u.a. über die Zwecke, Rechtsgrundlagen und Löschfristen).
- Soweit die betroffene Person nicht schon über die Informationen verfügt, ist sie
 - bei Direkterhebung zum Zeitpunkt der Erhebung zu informieren.
 - bei Dritterhebung spätestens innerhalb eines Monats.
- Bei den Informationspflichten handelt es sich um eine Bringschuld des Verantwortlichen!

RECHT AUF INFORMATION: INHALTE

- Name und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
- aus welcher Quelle die personenbezogenen Daten stammen (bei Dritterh.)
- die Zwecke sowie Rechtsgrundlage der Verarbeitung
- ggfls. die verfolgten berechtigten Interessen
- ggfls. die Empfänger der personenbezogenen Daten
- ggfls. beabsichtigte Drittlandübermittlung und Rechtsgrundlage dafür
- Betroffenenrechte
- Jederzeit mögliche Widerrufbarkeit der Einwilligung
- Beschwerderecht bei der Aufsichtsbehörde
- Dauer der Datenspeicherung, falls dies nicht möglich ist, die Kriterien für die Festlegung der Dauer

RECHT AUF INFORMATION: ART DER ERTEILUNG

- Der Verantwortliche ist bezüglich aller Betroffenenrechte verpflichtet, die Informationen in präziser, transparenter, verständlicher, leicht zugänglicher Form sowie in einer klaren und einfachen Sprache zu übermitteln.
- Dies kann schriftlich, in anderer Form, gegebenenfalls auch elektronisch erfolgen.

RECHT AUF INFORMATION: AUSNAHMEN

- Die DSGVO sieht einige Ausnahmen von den Informationspflichten vor, u.a. müssen die Informationen
 - bei Direkt- und Dritterhebung nicht erteilt werden, wenn und soweit die betroffene Person bereits über die Informationen verfügt.
 - bei Dritterhebung nicht erteilt werden, wenn die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde.

RECHT AUF INFORMATION: ADRESSAT DER INFORMATION

Grundsätzlich sind alle natürlichen Personen zu informieren, deren personenbezogene Daten Sie verarbeiten, u.a.:

- Webseitennutzer
- Mitarbeiter
- Kunden
- Probanden
- Veranstaltungsteilnehmer
- Aufgezeichnete Personen
- Nutzer bestimmter Anwendungen (Videokonferenzsystem, Cloud-Dienste, Raumreservierungssystem...)

RECHT AUF INFORMATION: BSP. VIDEOÜBERWACHUNG

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:

Kontaktadressen 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.

Beispiel für ein vollständiges Informationsblatt (Aushang) nach Art. 13 der Datenschutz-Grundverordnung bei Videoüberwachung¹

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 Empfängern 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 schutzwichtige 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 A4 erfolgen.

Quelle: Datenschutzaufsicht Niedersachsen

AGENDA

- Warum ist Datenschutz wichtig?
- Was beschäftigt Organisationen seit Anwendbarwerden der DSGVO?
 - Dokumentieren
 - Informieren
 - Löschen

SPEICHERBEGRENZUNGSGRUNDSATZ

- Art. 5 Abs. 1 lit. e DSGVO:

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist [....].

→ Löschung der die Person identifizierenden Merkmale.

→ z. B. bei pseudonymisierten Daten Löschung der getrennt gespeicherten Zuordnungsmerkmale.

- Konkretisierung wird der Grundsatz der Speicherbegrenzung u. a. in Art. 17 DSGVO (Recht auf Löschung bzw. Vergessenwerden).

- Sowohl vom Speicherbegrenzungsgrundsatz, als auch vom Recht auf Löschung gibt es Ausnahmen, die vor einer Löschung berücksichtigt werden müssen!

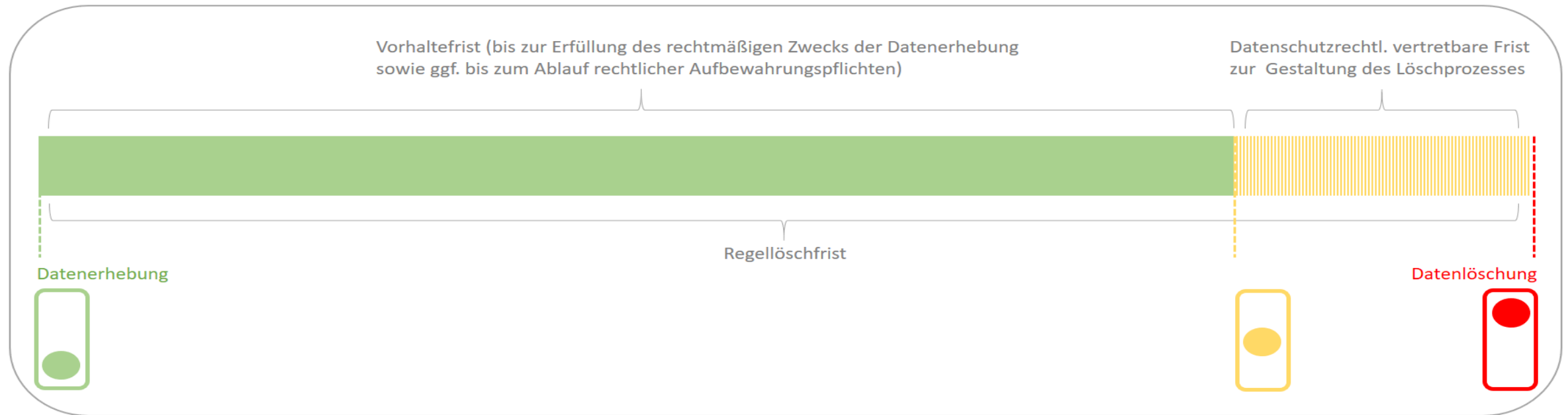
AUFBEWAHRUNGSPFLICHTEN

Dokumente	Aufbewahrungsfrist	Rechtsgrundlage
Empfangene Handels- und Geschäftsbriefe, Kopien der abgesandten Briefe und sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind	6 Jahre	§ 147 AO und §§ 238, 257 HGB
Bücher und Aufzeichnungen inkl. Handelsbücher, Inventare, Jahresabschlüsse, Bilanzen und die zu ihrem Verständnis erforderlichen Organisationsunterlagen (z. B. Vermerke), ausgestellte und empfangene Rechnungen, Buchungsbelege, Jahresabschlüsse, Einzelabschlüsse, Konzernabschlüsse, und sonstige Organisationsunterlagen	10 Jahre	§ 147 AO und §§ 238, 257 HGB

(und viele, viele mehr)

- Weitere Aufbewahrungspflichten können sich u.a. auch durch Kollektivvereinbarungen, Verjährungsfristen oder durch eine „akute“ Rechtsstreitigkeit ergeben!
- Solange rechtliche Aufbewahrungspflichten bestehen, wird der Grundsatz der Speicherbegrenzung ausgesetzt.

DIN-NORM 66398



Quelle: Angelehnt an DIN-Norm (stark vereinfachte Darstellung).

BEISPIELHAFTE LÖSCHREGEL

Vorfalldokumentation	
Inhaltl. Umfang	Die Löschregel umfasst alle Datenobjekte, die im Rahmen des Vorfallmanagement gespeichert werden, um Vorfälle ab deren Meldung zu bearbeiten.
Verwendungszwecke	<ul style="list-style-type: none">- Bearbeitung des Vorfalls,- ggf. Erfüllung von Melde- und Benachrichtigungspflichten,- ggf. Ergreifen von Schutzmaßnahmen zur Verhinderung von Folgeschäden,- Rechenschaftspflichten und Beweissicherung<ul style="list-style-type: none">o Art. 5 Abs. 2 DSGVO i.V.m. § 195 BGB, § 31 Abs. 2 Nr. 1 OWiG,o § 12 ProdHaftG.
Zeitraum bis zur vollständigen datenschutzrecht. Zweckerreichung	Vollständiger Abschluss der Vorfallbearbeitung und Ablauf aller relevanter Verjährungsfristen (i.d.R. nach 3 Jahren ab dem Ende des Jahres, in dem der Anspruch entstanden ist).
Aufbewahrungspflichten	-
Frist zur Umsetzung der Löschung	1 Jahr

Quelle: Rudolph/Selzer/Pordesch, BvD-News 02/21; angelehnt an DIN-Norm (stark vereinfachte Darstellung).

LÖSCHEN BEI AUFTRAGSVERARBEITUNG

- Im Falle einer Auftragsverarbeitung (z.B. Cloud-Speicherdienste, datenschutzkonforme Papierentsorgung, Systemwartungen) hat der Verantwortliche dem Auftragsverarbeiter die für die im Auftrag verarbeiteten Daten relevanten Löschregel(n) zu nennen.
- Insbesondere ist der Auftragnehmer zu verpflichten nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten zu löschen oder zurückzugeben und die vorhandenen Kopien zu löschen (nach Wahl des Verantwortlichen).
- Der Verantwortliche sollte sich die vollständige Löschung/Zurückgabe schriftlich bestätigen lassen.

QUELLENVERZEICHNIS (AUSWAHL)

- DIN-Norm 66398.
- Gola, Datenschutz-Grundverordnung, 2. Auflage 2018, C.H. Beck , München.
- Jandt/Steidle, Datenschutz im Internet, 1. Auflage 2018, Nomos, Baden Baden.
- Kühling/Buchner, DS-GVO BDSG, 3. Auflage 2019, C.H. Beck , München.
- Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, C.H. Beck, München.
- Rudolph/Selzer/Pordesch, Datenschutzkonformes Löschen bei Datenschutz- und Informationssicherheitsvorfällen, BvD-News 02/21, S. 36-41.
- Tinnefeld/Buchner/Petri/Hof, Einführung in das Datenschutzrecht, 6. Auflage 2018, Walter de Gruyter, Berlin/Boston.

Abbildungen: www.openclipart.org (Abruf vor Einstellung des Dienstes).

Vielen Dank für Ihre Aufmerksamkeit!

Dieser Vortrag wurde vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.