Grundlagen DSGVO für die Mitglieder der Österreichische Gesellschaft für Landschaftsplanung und Landschaftsarchitektur (ÖGLA)

Dr. iur. Heidi Scheichenbauer
Senior Researcher | Senior Consultant
heidi.scheichenbauer@researchinstitute.at

Research Institute AG & Co KG
Digital Human Rights Center
Smart Rights Consulting

Annagasse 8/1/8
1010 Wien
www.researchinstitute.at

Dr. iur. Heidi Scheichenbauer

- Juristin
- **Senior Researcher** und **Senior Consultant**, Research Institute
- Autorin von Fachbeiträgen in datenschutzrechtlichen Fachzeitschriften (Jus-IT, Datenschutz-konkret)
- Mitautorin mehrerer aktueller Bücher zur Datenschutz-Grundverordnung (jusIT Spezial: DS-GVO, Handbuch Datenschutz Verlag WEKA) Vortragstätigkeiten
- In Progress: Datenschutz für Vereine (Verlag Linde, Erscheinungsdatum Herbst/Winter 2018)
- **Erfahrungen** in:
  - Wissenschaft (RI, KMU Forschung Austria)
  - Öffentlichkeitsarbeit (Fundraising Verband Austria)
  - Rechtsberatung
- **Forschungsschwerpunkte**:
  - Telekommunikationsrecht

research institute

- Das **Research Institute (RI)** ist ein Forschungszentrum an der Schnittstelle von **Technik, Recht** und **Gesellschaft**, das sich aus multi- und interdisziplinärer Perspektive mit der Bedeutung der Menschenrechte im digitalen Zeitalter beschäftigt.
- **Portfolio:**

- **Forschung zu technischen** und **rechtlichen** Aspekten von **Datenschutz** und **Datensicherheit, Cybercrime, Technikfolgenabschätzung** und **Netzpolitik**
- **Smart Rights Consulting:** Beratung zu rechtlichen, technischen und organisatorischen Fragen des Datenschutzes
- **Schulungen**, auf Wunsch zugeschnitten auf Ihre Organisationen
- **Maßgeschneiderte technische Lösungen** zur praktischen Umsetzung der Compliance-Prozesse (in Zusammenarbeit mit Software-Entwicklern)
- **Konzeption und Durchführung individueller und multidisziplinärer Projekte** mit renommierten Partnern auf nationaler und internationaler Ebene.

Datenschutz – Worum geht es?

Allgemeines zur DSGVO

Datenschutz – Worum geht es?

- Primär geht es nicht um den Schutz von Daten vor den Menschen (vor Zerstörung, Diebstahl etc..).
- Das Grundrecht der Menschen auf Privatsphäre innerhalb der Informationsgesellschaft ist zu schützen.

Die europäischen Rechtsgrundlagen der DSGVO

Das Recht auf Privatleben:

- EMRK (1950) Artikel 8 (1) *„Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.“*

Das Recht auf Schutz der personenbezogenen Daten:

- Artikel 16 AEUV (1) und Artikel 8 EU Grundrechte-Charta: *„Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.“*

PERSONENBEZOGENE DATEN

- alle Informationen, die sich auf eine identifizierte/identifizierbare **natürliche Person** (der Betroffene) beziehen
- identifizierbar ist eine Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer (SV-Nummer), mit Online-Kennung identifiziert werden kann...
- =alles was eine Person identifizieren kann

PERSONENBEZOGENE DATEN

- Neu: nach DSGVO **kein Schutz für juristische Personen**
  - Somit sind Name, Rechtsform oder Kontaktdaten der jur. Person nicht geschützt (zB Office-Adresse)
  - Nationale Rechtslage nicht eindeutig– Verfassungsbestimmung des DSG wurde nicht aufgehoben
  - In Erläuterungen zum DSG: jur. haben Personen kein Recht auf Datenschutz

- Datenschutz jedoch jedenfalls weiterhin für:
  - natürliche Personen die für jur. Personen arbeiten

    (zb heidi.scheichenbauer@researchinstitute.at vs. office@researchinstitute.at)
  - Einzelunternehmer die natürliche Personen sind

PERSONENBEZOGENE DATEN

identifizierbare natürliche **Person**

- ErwG 26: es sollten *“alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach alllgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren”*
- Kommt nicht nur auf Wissen und Mittel des Verantwortlichen an, sondern auch Wissen und Mittel Dritter
- Ausreichend wenn Personenbezug durch irgendjemanden hergestellt werden kann

PERSONENBEZOGENE DATEN

- „identifiziert werden kann“ ist somit weit zu verstehen
- identifizierbare **natürliche Person** jedenfalls:
  - Kontodaten
  - Werbe-Cookie auf einem Computer samt darin gespeicherter Daten
  - IP-Adressen
  - Fotos (auf Website, Broschüren)….
- Kein Recht auf Datenschutz für verstorbene Personen (!)
- Datenverarbeitungen für den rein persönlichen/familiären Gebrauch sind von DSGVO ausgenommen

Verarbeitung personenbezogener Daten

- Verarbeitungsbegriff umfassend
- Insbesondere:

  *…..Erheben, Erfassen, Organisation, Ordnen, **Speicherung**, Anpassung, Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung, Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich, Verknüpfung, Einschränkung, Löschen oder die Vernichtung…*

- Auch das bloße E-Mail im Posteingang ist bereits eine Verarbeitung

Datenschutz-Prinzipien die einzuhalten sind

- Rechtmäßigkeit (Rechtsgrundlage erforderlich)
- Fair (bei Interessenabwägung wichtig)
- Transparent (für Betroffene nachvollziehbarer Weise)
- Zweckbindungsgrundsatz (Datenverwendung für bestimmte Zwecke)
- Datenminimierung (nur so viel verarbeiten wie erforderlich)
- Richtigkeit (Fehlerkorrektur wenn unrichtig)
- Speicherbegrenzung (nur so lange wie erforderlich personenbezogen speichern)
- Integrität und Vertraulichkeit
- Rechenschaftspflicht (Nachweis der Einhaltung)

ZIELE/AUSWIRKUNGEN DER DSGVO

- Stärkung der Betroffenenrechte
- Mehr Eigenverantwortung der Datenverarbeiter (Verantwortlicher und Auftragsverarbeiter)
- Größere Harmonisierung im europ. Raum
- Erweiterter Anwendungsbereich durch Marktortprinzip betrifft auch nicht EU-Anbieter die in EU anbieten (zB Facebook, Google, Amazon…)
- Höhere Strafen als bisher
- Auch Schadenersatzklagen möglich

Sanktionen nach der DSGVO(Hinweis: Verwarnungen ebenfalls möglich bzw. „vorgeschrieben“)

Delikt	neue Höchststrafe	bisherige Strafe
Missachtung Bescheid d. DSB	€ 20.000.000,– oder 4 % v.Ums.	€ 25.000
Verletzung des Auskunftsrechts	€ 20.000.000,– oder 4 % v.Ums.	€ 500
Verletzung der Löschungsrechts	€ 20.000.000,– oder 4 % v.Ums.	€ 500
unrechtmäßige Datenspeicherung	€ 20.000.000,– oder 4 % v.Ums.	€ 10.000
unzulässige Auslandsübermittlung	€ 20.000.000,– oder 4 % v.Ums.	€ 10.000
fehlender Datenschutzbeauftragter	€ 20.000.000,– oder 4 % v.Ums.	nicht strafbar
Nichtvornahme DSFA/DPIA	€ 10.000.000,– oder 2 % v.Ums.	nicht strafbar
mangelhafte Datensicherheit	€ 10.000.000,– oder 2 % v.Ums.	€ 10.000
kein Verarbeitungsverzeichnis	€ 10.000.000,– oder 2 % v.Ums.	€ 10.000,–
fehlende Elternzustimmung	€ 10.000.000,– oder 2 % v.Ums.	nicht strafbar
Nicht-Kooperation mit DSB	€ 10.000.000,– oder 2 % v.Ums.	nicht strafbar

Wer haftet für Geldbußen?

- Primär jur. Person (zB Verein, GmbH, AG…)
- Alternativ kann Behörde Geldbuße gegen Mitglieder der Geschäftsleitung verhängen
- Nach § 9 Verwaltungsstrafgesetz kann auch ein verantwortlicher Beauftragter bestellt werden
- Grundsätzlich one-size-fits-all Zugang (zB keine Erleichterungen für Vereine)

Unterschiedliche Pflichten für Verantwortliche/Auftragsverarbeiter

- Betroffenenrechte (Verantwortlicher)
- Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung (Verantwortlicher)
- Verzeichnis von Verarbeitungstätigkeiten (Verantwortlicher und Auftragsverarbeiter)
- Meldung von Datenschutzverletzungen (Verantwortlicher)
- Datenschutz-Folgenabschätzung (Verantwortlicher)
- Verpflichtender Datenschutzbeauftragter (kann Verantwortlichen und/oder Auftragsverarbeiter betreffen)
- Datensicherheitsmaßnahmen (Verantwortlicher und Auftragsverarbeiter)

Verantwortliche/Auftragsverarbeiter - Abgrenzung

- „Verantwortlicher“ nat. oder jur. Person die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet
  - idR das Landschaftsarchitekturbüro
- „Auftragsverarbeiter“ eine nat. oder jur. Person die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet
  - zB verschiedene e-mail-Dienstleister (Mailchimp)/Druckerei/Google (Webanalyse-Tools)
- Auftragsverarbeitervereinbarung zwischen V und A erforderlich (schriftlich/elektronisch – Anpassung bestehender Verträge erforderlich)

Gemeinsam für die Verarbeitung Verantwortliche

Zwei oder mehr Verantwortliche legen gemeinsam

- Zwecke
- und Mittel zur Verarbeitung fest
- zB häufig bei gemeinsam betriebenen/gepflegten Datenbanken

Vereinbarung muss geschlossen werden, darin ist festzulegen

- wer welche Verpflichtung erfüllt
- insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und
- wer welchen Informationspflichten nachkommt

Wichtige Rechtsgrundlagen nach der DSGVO

Für Verarbeitungstätigkeiten

Rechtmäßigkeit ist u.a. dann gegeben (Häufigste RGL)

- Für **Vertragserfüllung** erforderlich
- **Einwilligung** (für einen oder mehrere bestimmte Zwecke)
- Verarbeitung ist zur Wahrung der **berechtigten Interessen** des Verantwortlichen erforderlich und das Interesse des Betroffenen überwiegt nicht
- Erfüllung rechtlicher Verpflichtungen (zB AN-Anmeldung)

VERTRAGSERFÜLLUNG

- Verarbeitung auf dieser Rechtsgrundlage ist zulässig, wenn…
  - Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei der Betroffene
  - oder zur Durchführung vorvertraglicher Maßnahmen (die auf Anfrage des Betroffenen erfolgen)
- erforderlich ist

Betrifft insbesondere…

- Lieferanten (Kontaktpersonen)
- Kunden (Kontaktpersonen)

EINWILLIGUNG I

- freiwillig (zu verschiedenen Verarbeitungsvorgängen muss Einwilligung jeweils gesondert möglich sein)
- für den bestimmten Fall (pauschale Einwilligung ohne Zweckangabe nicht zulässig)
- in informierter Weise (Kenntnis von Verantwortlichen, Zweck, Hinweis auf Widerrufsmöglichkeit, Datenkategorien, Übermittlungsempfänger)
- Einwilligung muss nachgewiesen werden können (Rechenschaftspflicht)

EINWILLIGUNG II

- Grunds. keine Formvorschriften
  - Verwendung von vorangekreuzten Opt-In Boxen unzulässig
  - Schweigen ist keine Zustimmung
- Klare und einfache Sprache (für Durchschnittsbetroffenen verständlich)
- Nicht versteckt (etwa in „AGB“ wenn dann „AGB und Datenschutzbestimmungen“) = leicht zugänglich
- Einwilligung muss als solche bezeichnet werden
  - *Nicht….“mir ist bekannt, dass…“*
  - *Sondern ….“ ich willige in die Verarbeitung meiner Daten ein…“*
- Einwilligung gilt zeitlich unbeschränkt
- Einwilligung muss leicht widerrufbar sein

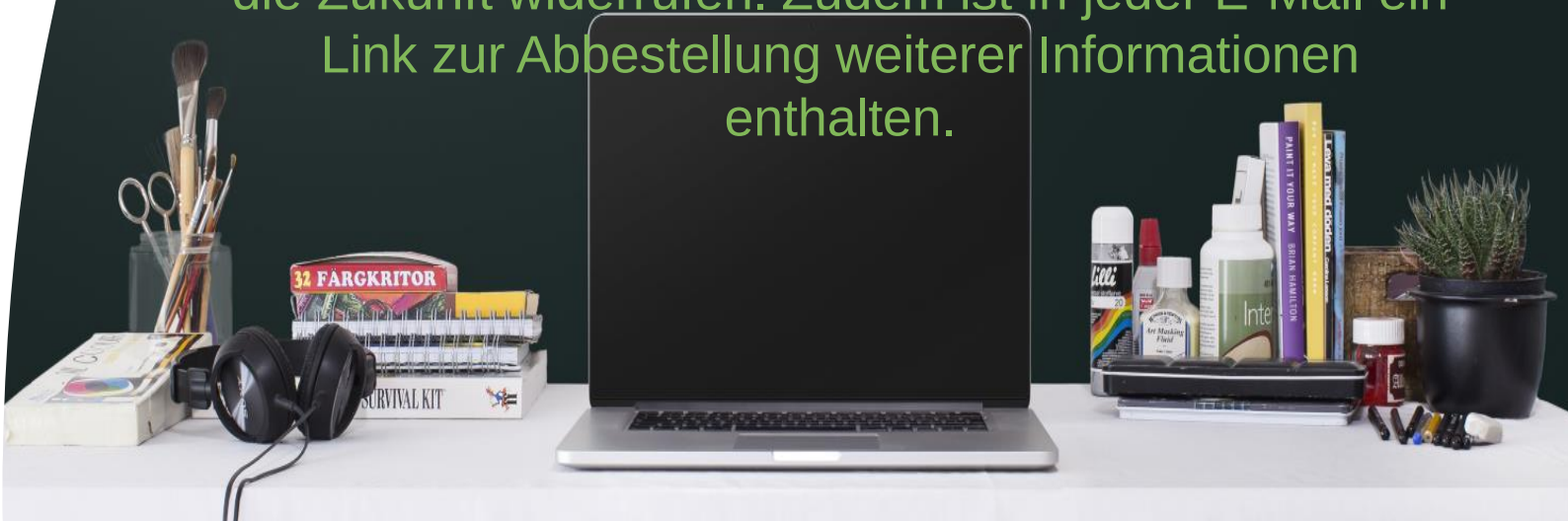
research institute

Eine solche Einwilligungserklärung ist unwirksam, da hier nicht ersichtlich ist, welche Medien (E-Mail, SMS, Telefon, Brief) für die Werbung verwendet werden sollen.

Ich willige in die Nutzung meiner Daten für Werbung ein. Meine Einwilligung kann ich jederzeit per E-Mail an unsubscribe@ abc.de widerrufen.

research institute

Ich möchte den wöchentlichen Newsletter der ABC GmbH mit Informationen zu deren Angeboten aus dem Bereich Telekommunikation per E-Mail erhalten. Meine Daten werden keinesfalls an Dritte weitergegeben. Meine Einwilligung kann ich jederzeit per E-Mail an unsubscribe@ abc.de mit Wirkung für die Zukunft widerrufen. Zudem ist in jeder E-Mail ein Link zur Abbestellung weiterer Informationen enthalten.



BERECHTIGTE INTERESSEN

- Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich u. Interessen, Grundrechte, Grundfreiheiten des Betroffenen überwiegen nicht.
- Laut DSGVO kann sogar *…Direktwerbung… als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden…* (zB Verwendung von Daten für postalische Werbung)
- Zu berücksichtigen sind dabei:
  - Vernünftige Erwartungen des Betroffenen
  - Information des Betroffenen wesentlich für Erwartungshaltung
  - Betroffener hat (wie bei Einwilligung) jedenfalls eine jederzeitige Untersagungsmöglichkeit

Exkurs (Wichtig!): Berechtigtes Interesse und Werbung

- berechtigtes Interesse rechtfertigt nicht die Versendung von e-mails und „cold-calling“
- Telefon und E-Mail-Kontaktaufnahme sind in § 107 Telekommunikationsgesetz geregelt (nicht in der DSGVO)

Für e-mails/Telefonanrufe gilt:

- Grundsätzlich Einwilligung erforderlich
- Opt-Out bei E-Mails wenn bereits e-mail Kontakt bestanden hat (so lange bis der Empfänger untersagt).

ZWECKBINDUNG NEU I

- Kann ich Daten die nur für einen Zweck (zB Auftrag) für anderen Zweck (zB Werbung) verwenden?
- Grundsätzlich muss **zum Erhebungszeitpunkt** eindeutiger und legitimer **Zweck** festgelegt werden.
- Nach DSGVO Daten dürfen zu Zwecken weiterverarbeitet werden die mit ursprünglichen Zwecken vereinbar sind.

Zu berücksichtigen sind folgende Kriterien:

- Verbindung zwischen ursprünglichen und neuen Zweck.
- Art der personenbezogenen Daten (werden „sensible“ Daten verarbeitet)?
- mögliche Folgen der beabsichtigten Weiterverarbeitung für Betroffene

PROFILING I

…jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese ***personenbezogenen Daten verwendet*** *werden, um bestimmte* ***persönliche Aspekte****, die sich auf eine natürliche Person beziehen,* ***zu bewerten****, insbesondere um Aspekte bezüglich Arbeitsleistung,* ***wirtschaftliche Lage****, Gesundheit, persönliche Vorlieben,* ***Interessen****, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu* ***analysieren*** *oder vorherzusagen…*

- sehr umfassender Begriff
- Einordnung in Marketing-Zielgruppe fällt darunter

PROFILING II

Nach DSGVO unterschiedliche Arten des Profilings

- Profiling zu rein internen Zwecken (zB ob Lieferanten zuverlässig sind, Bonitätsauskünfte zu internen Zwecken)
- Profiling zu Marketingzwecken
- Profiling mit rechtlichen Folgen oder ähnlicher schwerer Eingriffsintensität (kritisches Profiling)
- Profiling auf Basis von sensiblen Daten/erhöhter Eingriffsintensität (kritisches Profiling)

PROFILING III

Keine Zustimmung (Opt-In) für folgende Profiling-Arten erforderlich…

- Profiling für rein interne Zwecke (berechtigtes Interesse als RGL möglich)
- Profiling zu Marketingzwecken (berechtigtes Interesse als RGL möglich)
- Bei Datenerhebung Informationserteilung wichtig (!)
- Betroffener muss wissen was mit Daten gemacht wird
- Stets Widerspruch (Opt-Out) des Betroffenen möglich

ZUSAMMENFASSUNG I

Handlungsbedarf:

- Zwecke und Rechtsgrundlagen definieren
- Auf welche Rechtsgrundlagen kann ich meine Datenverarbeitungen stützen?
- Wenn berechtigtes Interesse als RGL, dokumentieren, warum man glaubt berechtigtes Interesse zu haben

research institute

ORGANISATORISCHE PUNKTE

Wichtig organisatorische Anforderungen sind insbesondere:

- Verzeichnis der Verarbeitungstätigkeiten
- Datenschutzbeauftragter
- Datenschutz-Folgenabschätzung
- Datensicherheitsmaßnahmen

Verzeichnis von Verarbeitungstätigkeiten

Verarbeitungstätigkeit in DSGVO nicht näher definiert. Entspricht im Wesentlichen der Datenanwendung iSd alten DSG 2000:

- *Verarbeitungstätigkeit ist die Summe aller Datenverarbeitungen, die für einen bestimmten Zweck oder für mehrere miteinander zusammenhängende Zwecke durchgeführt werden, können als eine Verarbeitungstätigkeit verstanden werden.*

Verzeichnis von Verarbeitungstätigkeiten (1)

- „KMU-Ausnahme“ (= Entfall) wenn weniger als 250 Mitarbeiter
- Pflicht zur Führung von Verarbeitungsverzeichnissen besteht dennoch:
  - Verarbeitung birgt Risiken für betroffene Personen, oder
  - **Verarbeitung erfolgt nicht nur gelegentlich**, oder
  - sensible Daten werden verarbeitet

- Wohl wenige Ausnahmen, da Datenverarbeitungen zumeist öfter als regelmäßig erfolgen.
- Aufzeichnungen können schriftlich oder elektronisch (Word, Excel etc.) erfolgen.

Verzeichnis von Verarbeitungstätigkeiten (2)

- Betrifft „Verantwortliche“ (= Auftraggeber **UND** Auftragsverarbeiter (=Dienstleister)
- Inhalt ist ähnlich den DVR-Meldungen, insbesondere
  - Name und Kontaktdaten des Verantwortlichen und eines etwaigen Datenschutzbeauftragten
  - Verarbeitungszwecke
  - Kategorien betroffener Personen, personenbezogener Daten und Empfänger
  - Informationen zu Datenübermittlungen in Drittländer
  - Speicherdauer
  - Datensicherheitsmaßnahmen
- Ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen

DATENSCHUTZBEAUFTRAGTER

- (Wann) ist ein Datenschutzbeauftragter zu bestellen?
  - Keine allgemeine Pflicht
  - Kerntätigkeit muss
    - in Verarbeitungsvorgängen, welche … *eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich macht,*
    - ist Verarbeitung von besonderen Datenarten (zB Krankheitsdaten/politische Daten) im umfangreichen Ausmaß bestehen
  - Keine Definitionen von “Kerntätigkeit” und “systematischer Überwachung” und “umfangreich” in DSGVO
  - Für ÖGLA Mitglieder wohl nicht relevant
  - Ernennung eines Datenschutz-Koordinators empfehlenswert

DATENSCHUTZ-FOLGENABSCHÄTZUNG

Wenn auf Grund von Art, Umfang, Umständen und Zwecke der Verarbeitung voraussichtlich ein hohes DS-Risiko besteht, **insbesondere** bei:

- systematischer und umfassender Bewertung persönlicher Aspekte von Personen erfolgt (v. a. Profiling) wenn Ergebnis Entscheidungsgrundlage mit (Rechts)wirkungen gegenüber Personen bildet (z.B. bei der Frage, ob ein Kredit gewährt wird)
- bei einer umfangreichen Verarbeitung sensibler Daten bzw. strafrechtlicher Inhalt,
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

DATENSCHUTZ-FOLGENABSCHÄTZUNG (2)

- Laut Guidelines der Artikel 29 Gruppe: zusätzlich 9 Kriterien berücksichtigen - wenn 2 davon erfüllt, soll DSFA erfolgen
- Häufig vorliegende Kriterien:
  - Bewerten oder Einstufen („Scoring“)
  - Verarbeitung vertraulicher Daten oder höchst persönlicher Daten (zB, politische Einstellung, Weltanschauung, aber auch „sehr persönliche Daten“, Finanzdaten, die für den Zahlungsbetrug missbraucht werden könnten)
  - Datenverarbeitung in großem Umfang (großer Umfang nicht definiert)
  - Abgleichen oder Zusammenführen von Datensätzen aus unterschiedlichen Datenbeständen (zum Zwecke des Profilings)

DATENSCHUTZ-FOLGENABSCHÄTZUNG (3)

- Die Datenschutzbehörde hat White-List für Fälle erstellt, in denen keine DFA erforderlich ist.
- Häufige Anwendungen (Personalverwaltung, Kundenverwaltung, Mitgliederverwaltung, Marketing) sind enthalten.
- Die Datenschutzbehörde wird Black-List für Fälle erstellen, in denen eine DSFA erforderlich ist.
- DSFA für ÖGLA Mitglieder wohl nicht relevant

BETROFFENENRECHTE

u. a.:

- Informationsrechte
- Auskunftsrecht
- Datenübertragbarkeit
- Recht auf Löschung
- Widerspruch
- Einschränkung der Verarbeitung
- Berichtigung
- Grds. haben sich vorwiegend die Modalitäten geändert

Worüber muss der Betroffene informiert werden (1)

u.a über:

- Namen + Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten (wenn vorhanden)
- die Zwecke und Rechtsgrundlage für Verarbeitung
- wenn die Verarbeitung auf Grund von berechtigten Interessen, die berechtigten Interessen
- Empfänger der personenbezogenen Daten (auch dass DL eingesetzt wird)
- die Absicht des Verantwortlichen Daten an ein Drittland zu übermitteln (häufig bei Cloud-Lösungen oder E-Mail-Versendern wie zB Mailchimp)

Worüber muss der Betroffene informiert werden (2)

- das Bestehen „ihrer Rechte“ (Auskunft, Löschung, Widerruf, Datenübertragbarkeit…etc.)
- Beschwerderecht bei DSB
- ob Daten aus rechtlichen Gründen (Gesetz/Vertrag) bereitzustellen sind (+allfällige Folgen der Nichtbereitstellung)
- Speicherdauer/ falls dies nicht möglich ist, die Kriterien für Dauer
- ob Weiterverarbeitung zu anderen Zwecken beabsichtigt ist

Wenn nicht vom Betroffenen erhoben (Adressenkauf) zusätzlich:

- Kategorien der verarbeiteten pb Daten
- Aus welcher Quelle Daten stammen (wenn genaue Quelle nicht bekannt, allgemeine Beschreibung)

Worüber muss der Betroffene informiert werden (3)

Wann/Wie?

- Zum Zeitpunkt der Erhebung der Daten vom Betroffenen
- Wenn nicht vom Betroffenen erhoben binnen 1 Monats

Keine Formvorschriften wie zu informieren ist:

- Theoretisch mündlich möglich
- Zu Beweiszwecken schriftlicher/elektronisch empfehlenswert
- Bei schriftlicher Erhebung Beilage mit Datenschutzerklärung, link auf Website mit Datenschutzerklärung, oder in e-mail-Signatur

Recht auf Auskunft

- Bestätigung ob und welche personenbezogene Daten verarbeitet werden
- Verarbeitungszwecke, Datenkategorien, Empfänger (Adressdaten, Namensdaten…)
- geplante Speicherdauer (falls unmöglich Kriterien für die Festlegung dieser Dauer – wie lange werden Daten gespeichert)
- Bestehen eines Rechts auf Berichtigung/Löschung/Einschränkung der Verarbeitung durch den Verantwortlichen /Widerspruchsrechts
- Beschwerderecht
- Binnen eines Monats (kann auf 2 Monate erstreckt werden)
- wenn Daten nicht beim Betroffenen erhoben, alle verfügbaren Informationen über die Herkunft der Daten
- Unentgeltliche Kopie muss zur Verfügung gestellt werden

Recht auf Widerspruch

- Bei Datenverarbeitung auf Grund des berechtigten Interesses (zB für Direktwerbung), hat der Betroffene, jederzeit Widerspruch gegen die Verarbeitung der Daten einzulegen (gilt auch für Profiling, wenn mit Direktwerbung in Verbindung)
- Verantwortlicher darf nicht weiterverarbeiten
- Person muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf das Recht hingewiesen werden

Recht auf Löschung

- Betroffener hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten **unverzüglich** gelöscht werden, wenn
  - Datenverwendung nicht mehr notwendig
  - Einwilligung wird widerrufen und anderweitige Rechtsgrundlage fehlt
  - Widerspruch gegen die Verarbeitung erfolgt
  - Daten wurden unrechtmäßig verarbeitet

- Kann die Berichtigung oder Löschung nicht unverzüglich erfolgen, so ist die Verarbeitung einzuschränken (DS-AnpG 2018)

Recht auf Datenübertragbarkeit

Wenn Daten durch Einwilligung/Vertrag erhoben wurden

- gedacht für Social Media/Telekomunternehmen
- auch auf andere Verantwortliche anwendbar
- der Betroffene das Recht seine Daten in einem strukturierten, gängigen und maschinenlesbaren Format vom Verantwortlichen zu erhalten
- das Recht, diese Daten einem anderen Verantwortlichen zu übermitteln
- Direkte Übermittlung von einem Verantwortlichen zum anderen V, **soweit technisch machbar**

Meldepflicht von Datenschutzverletzungen

- **Verletzung des Schutzes personenbezogener Daten (Datenschutzverletzung)** ist jede Verletzung der Sicherheit, ob unbeabsichtigt oder unrechtmäßig, die zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt.
- Das reicht vom irrtümlichen Versand personenbezogener Daten an den falschen E-Mail-Empfänger über den Verlust personenbezogener Daten bis hin zum mutmaßlichen Hackerangriff.
- „Stufe 0“: kein Risiko - Keine Meldepflicht
- „Stufe 1“: Risiko
  Jede Datenschutzverletzung, die voraussichtlich zu einem **Risiko für die Betroffenen** führt, ist unverzüglich **an die Aufsichtsbehörde zu melden**, möglichst binnen 72 Stunden nachdem die Verletzung bekannt wurde (Verzögerungen sind zu begründen).
- „Stufe 2“: Hohes Risiko
  Über jede Datenschutzverletzung, die voraussichtlich zu einem **hohen Risiko für die Betroffenen** führt, sind zusätzlich unverzüglich **die Betroffenen zu informieren**.

Datensicherheit als Teil des Datenschutzes

Verantwortliche und Auftragsverarbeiter müssen **geeignete angemessene** Datensicherheitsmaßnahmen treffen. Das sind va:

- Verschlüsselung
- Fähigkeit der Sicherstellung der Sicherheit der Systeme
- Fähigkeit, Verfügbarkeit nach einem Zwischenfall rasch wiederherzustellen
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung
- Stand der Technik, Implementierungskosten, Risiken sind zu berücksichtigen

LAUFENDE MITARBEITERPFLICHTEN

Die DSGVO wird durch die Mitarbeiter umgesetzt: Jede Organisation ist darauf angewiesen, dass ihre Mitarbeiter **in ihrer täglichen Arbeit** die DSGVO einhalten und zur Erfüllung der DSGVO-Pflichten beitragen:

- **Dokumentation**
  Die Organisation führt ein **Verzeichnis von Verarbeitungstätigkeiten** personenbezogener Daten („Verarbeitungsverzeichnis“). Die Mitarbeiter haben dafür zu sorgen, dass jede neue oder geänderte Verarbeitung personenbezogener Daten in dieses Verzeichnis eingetragen wird.
- **Prüfung der Rechtmäßigkeit**
  Bei jedem Vorgang der Datenverarbeitung ist grundsätzlich zu prüfen, ob die beabsichtigte Verarbeitung von Daten rechtlich zulässig ist.
- **Informationspflicht**
  Der Betroffene ist grundsätzlich darüber zu informieren, wenn personenbezogene Daten über ihn verarbeitet werden (inkl. zahlreicher Details).
- **Datenvermeidung/Datensparsamkeit/Zweckbindung**
  Die Datenverarbeitung ist so zu organisieren, dass so wenig personenbezogene Daten wie möglich erhoben, gespeichert und verarbeitet werden.
- **Speicherbegrenzung/Löschung**
  Wenn personenbezogene Daten nicht mehr benötigt werden und etwaige gesetzlichen Aufbewahrungspflichten abgelaufen sind, sind diese zu löschen. Für die gespeicherten Daten ist festzulegen, für welchen Zeitraum eine Aufbewahrung bzw. Speicherung zu erfolgen hat. Gesetzliche Aufbewahrungspflichten sind hierbei zu beachten. Nach Ablauf der Aufbewahrungsfrist bzw. Speicherdauer ist für eine Löschung der Daten zu sorgen.

Besondere Mitarbeiterpflichten

Die DSGVO wird durch die Mitarbeiter umgesetzt: In **bestimmten Situationen** müssen Sie in der Lage sein, den Datenschutzbezug zu erkennen, und entsprechend zu handeln.

- **Meldepflicht von Datenschutzverletzungen**
  Jede Verletzung des Schutzes personenbezogener Daten (das reicht vom irrtümlichen Versand personenbezogener Daten an den falschen E-Mail-Empfänger, über den Verlust personenbezogener Daten bis hin zum mutmaßlichen Hackerangriff) ist **schnellstmöglich an die IT-Abteilung zu melden**. Meldungen von Sicherheitsvorfällen werden stets positiv gewertet.
- **Anfragen von Betroffenen (Betroffenenrechte)**
  Anfragen von Betroffenen zur Geltendmachung ihrer Rechte auf Auskunft, Berichtigung, Löschung, Widerruf, Widerspruch oder Datenübertragbarkeit sowie Beschwerden im Zusammenhang mit dem Umgang mit personenbezogenen Daten sind **schnellstmöglich zu behandeln. Vertretungsregelungen wichtig.**
- **Einführung neuer Systeme**
  Der Datenschutz ist von Anfang an in die Spezifikationen und die Architektur von Datenverarbeitungssystemen zu integrieren, um die Einhaltung der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes zu erleichtern („Privacy by Design“).

Mitarbeiterpflichten zur Datensicherheit (1/2)

Die DSGVO wird durch die Mitarbeiter umgesetzt: Folgende Pflichten bestehen zur Gewährleistung einer angemessenen Datensicherheit

- **Schutz vor unbefugtem Zugriff**
  - Werden Geräte unbeaufsichtigt gelassen, so ist sofort die Bildschirmsperre zu aktivieren.
  - Nicht besetzte Büroräumlichkeiten sind abzuschließen.
- **Sichere Datenspeicherung**
  - Daten sind derart zu speichern, dass die Verfügbarkeit und damit auch die Wiederherstellbarkeit im Schadensfall gewährleistet ist. Dies ist grundsätzlich bei zentralen Systemen (wie z.B. Netzlaufwerke) sichergestellt. Nicht sichergestellt ist dies bei dezentralen System (wie z.B. lokal auf den Endgeräten).
  - Im Zweifelsfall hat der Benutzer die IT-Abteilung zu kontaktieren.
- **Sichere Datenweitergabe**
  - Bei der Weitergabe von Daten ist ihr Schutzbedarf zu beachten und eine geeignete Versandart zu wählen. Wenn es der Schutzbedarf erfordert, sind diese nur in verschlüsselter Form weiterzugeben. Vertrauliche und sicherheitsrelevante Daten sind jedenfalls nur in verschlüsselter Form weiterzugeben.
  - Die Speicherung von Daten auf externen Datenträgern (wie z.B. USB-Sticks) darf nur dann erfolgen, wenn der Schutzbedarf der Daten nicht entgegensteht, wenn die Verfügbarkeit gewährleistet ist und soll auf das Minimum reduziert werden. Vertrauliche und sicherheitsrelevante Daten sind jedenfalls nur in verschlüsselter Form zu speichern.

Mitarbeiterpflichten zur Datensicherheit (2/2)

- **Richtiger Umgang mit Passwörtern**
  - Passwörter sind durch den Benutzer sicher auszuwählen. Ein sicheres Passwort ist mindestens acht Zeichen lang, enthält eine Mischung von Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen und ist nicht erratbar.
  - Passwörter sind geheim zu halten. Die Weitergabe von persönlichen Passwörter an andere Personen ist untersagt.
  - Ein Passwort ist zu wechseln, wenn das Passwort unautorisierten Personen bekannt geworden ist oder der Verdacht besteht.
  - Passwörter dürfen nur in sicherer Art und Weise gespeichert werden (verschlüsselter Passwortmanager). Das Aufschreiben von Passwörtern (z.B. auf Papier) ist jedenfalls untersagt.
- **Richtiger Umgang mit Geräten**
  - Die automatische Installation von Updates darf nicht eingeschränkt oder verhindert werden. Sofern Updates durch den Benutzer zu erfolgen haben, müssen diese unverzüglich durchgeführt werden.
  - Voreingestellte Sicherheitskonfigurationen und Sicherheitssysteme dürfen nicht durch den Benutzer deaktiviert oder umgangen werden.

Bereich Smartphones/Laptops

- Häufig Speicherung von personenbezogenen Daten
- Kontaktdaten und E-Mails, Office Dokumente wie Word oder Excel, sowie auch PDFs
- Nur unbedingt benötigte Daten am Handy speichern
- So rasch wie möglich löschen
- Zugriffsschutz: Authentifizierung mittels Muster, Passwort oder biometrischen Merkmalen wie Fingerabdruck oder Gesichtserkennung.
- Verschlüsselung des Telefonspeichers, Entsperrung beim Start des Geräts, Virenschutz
- Sicherheitsmaßnahmen des Smartphones in Erfahrung bringen und einsetzen

Bereich Smartphones/Laptops

- Häufig Speicherung von personenbezogenen Daten
- Kontaktdaten und E-Mails, Office Dokumente wie Word oder Excel, sowie auch PDFs
- Nur unbedingt benötigte Daten am Handy speichern
- So rasch wie möglich löschen
- Zugriffsschutz: Authentifizierung mittels Muster, Passwort oder biometrischen Merkmalen wie Fingerabdruck oder Gesichtserkennung.
- Verschlüsselung des Telefonspeichers, Entsperrung beim Start des Geräts, Virenschutz
- Sicherheitsmaßnahmen des Smartphones in Erfahrung bringen und einsetzen

Nützliche Links

- Allgemeine Checkliste https://www.privacyofficers.at/Privacyofficers_Checkliste_Umsetzung_DSGVO_v2.0.pdf
- Muster Verfahrensverzeichnis: https://www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf
- Muster Auftragsverarbeitervereinbarung: https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/EU-DSG/170515-Auftragsverarbeitung-Anlage-Mustervertrag-online.pdf
- Leitfaden der Datenschutzbehörde: https://www.dsb.gv.at/documents/22758/116802/DSGVO-Leitfaden-2018.pdf/01c18811-eb9e-4293-a9f1-0464d5e22b8f
- Muster für technische und organisatorische Maßnahmen: https://www.datenschutz-guru.de/muster-fur-technische-und-organisatorische-massnahmen-zur-datensicherheit-nach-art-32-dsgvo/

Grundlagen DSGVO für die Mitglieder der Österreichische Gesellschaft für Landschaftsplanung und Landschaftsarchitektur (ÖGLA)

Dr. Heidi Scheichenbauer
Senior Researcher | Senior Consultant
heidi.scheichenbauer@researchinstitute.at

Research Institute AG & Co KG
Digital Human Rights Center
Smart Rights Consulting

Annagasse 8/1/8
1010 Wien
www.researchinstitute.at

RECHTLICHE HINWEISE

Zweck: Dieses Dokument dient als Trainingsunterlage.

Erstellt von: Ing. Mag. Dr. Christof Tschohl, Dipl.-Ing. Dr. Walter Hötzendorfer, Mag. Markus Kastelitz, Dr. Heidi Scheichenbauer

Kontaktdaten: heidi.scheichenbauer@researchinstitute.at