DSGVO

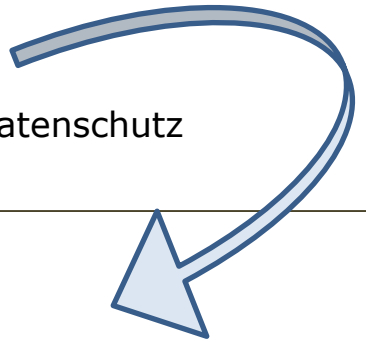
Einführung in das Datenschutzrecht

mit speziellem Fokus auf das Schulwesen in Österreich

Datenschutzrecht allgemein

Allgemeine Rechtsgrundlagen.

- Datenschutz ist ein **Grundrecht** in der EU
- Europäische Menschenrechtskonvention: Schützt Privatsphäre
- EU Grundrechtecharta: Schützt das Grundrecht auf Datenschutz
- Österreich: § 1 Datenschutzgesetz: Recht auf Privatsphäre und Datenschutz



EU Grundrechtscharta

- **Artikel 7 Achtung des Privat- und Familienlebens**

  Jede Person hat das **Recht auf Achtung ihres Privat- und Familienlebens**, ihrer Wohnung sowie ihrer **Kommunikation**.

- **Artikel 8 Schutz personenbezogener Daten**

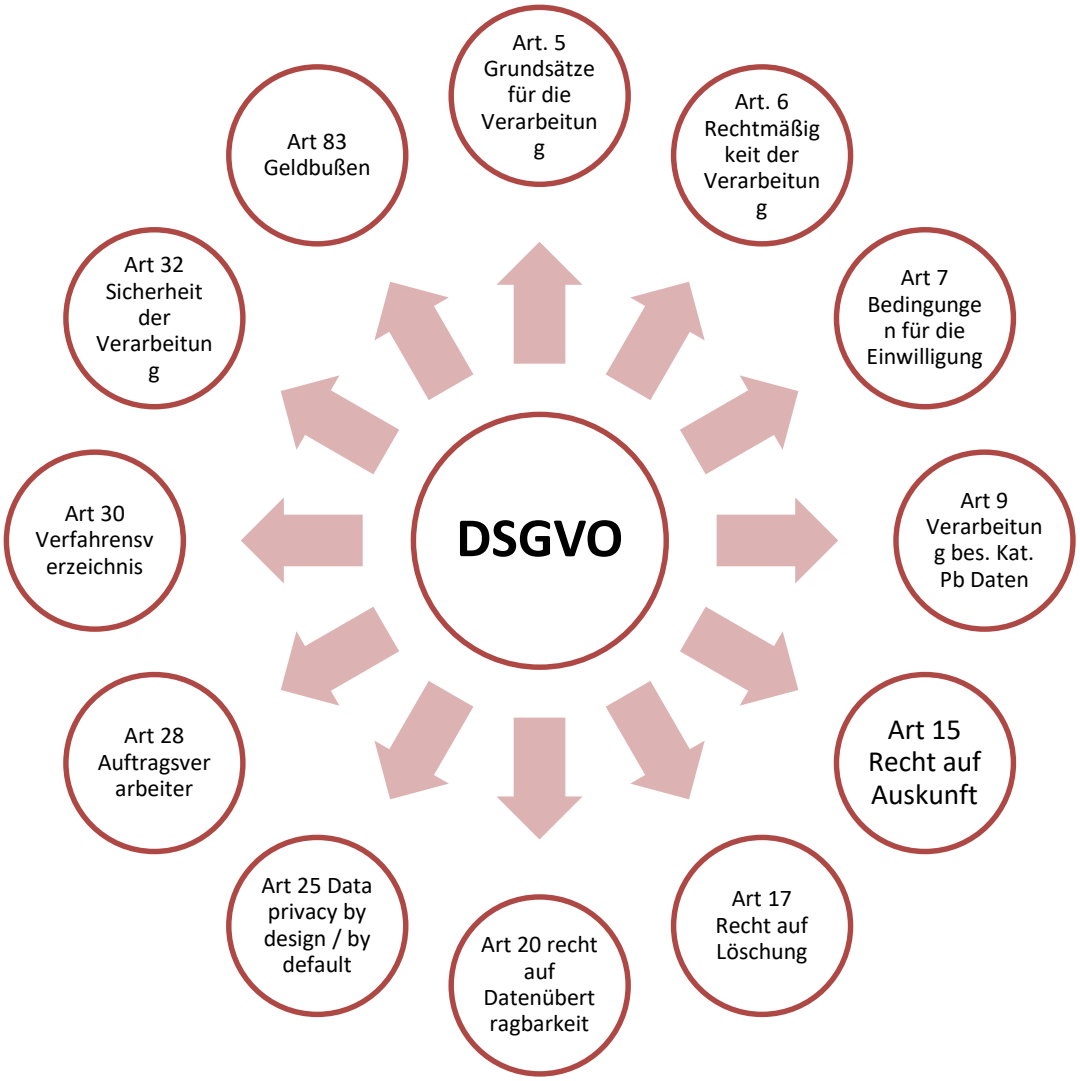
  (1) Jede Person hat das Recht auf Schutz der sie betreffenden **personenbezogenen Daten**.

  (2) Diese 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. Jede Person hat das Recht, **Auskunft** über die sie betreffenden erhobenen Daten zu erhalten und die **Berichtigung** der Daten zu erwirken.

  (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Die EU Datenschutzgrundverordnung.

konflikt&lösung



DSG – DSGVO voll anwendbar!

§ 11 DSG Verwarnung durch die Datenschutzbehörde

*§ 11. Die Datenschutzbehörde wird den Katalog des Art. 83 Abs. 2 bis 6 DSGVO so zur Anwendung bringen, dass die Verhältnismäßigkeit gewahrt wird. Insbesondere bei erstmaligen Verstößen wird die Datenschutzbehörde im Einklang mit Art. 58 DSGVO von ihren Abhilfebefugnissen insbesondere durch **Verwarnen** Gebrauch machen."*

Artikel 83 DSGVO: Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) *Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.*
*(2) **Geldbußen** werden je nach den Umständen des Einzelfalls **zusätzlich** zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt: ....*

Das DSG setzt Strafen der DSGVO in Ö NICHT außer Kraft

Ziele und Grundsätze der DSGVO

Grundsätze.

- Zweckbindung
- Rechtmäßigkeit
- Richtigkeit
- Verarbeitung nach Treu und Glauben, Transparenz
- Datenminimierung und Speicherbegrenzung
- Integrität und Vertraulichkeit
- Data Privacy by design/Data Privacy by Default
- Rechenschaftspflicht

Derjenige, der Daten verarbeitet muss stets nachweisen können, dass die DSGVO eingehalten wird!

Schutzziel.

- Schaffung einer **Balance** im Hinblick auf die **Grundrechtscharta** zwischen dem Menschen, seiner Privatsphäre und der Funktion von Datenschutz in der Gesellschaft.

- **<u>Datenschutzrecht nur für natürliche Personen;</u>**

Sanktionen.

- **Verwaltungsstrafen durch DSB**
  - Bis zu 20 Mio Euro oder 4 % des weltweiten jährlichen Konzernumsatzes des letzten Finanzjahres
  - Verwaltungsstrafverfahren gegen Unternehmen und/oder Geschäftsführung/§9 VstG Verantwortliche
  - Zusätzliche Verwaltungsstraftatbestände mit bis zu 50.000 Euro Strafdrohung (zB bei Verletzung des Datengeheimnisses gem § 11 DSG)
- **Gerichtsverfahren**
  - Unterlassung und Schadenersatz

Hohe Strafen, Reputationsverlust, Vertrauensverlust können existenzbedrohlich sein

Terminologie

Wichtige Begriffe.

Verantwortlicher	Verantwortlicher im Sinne der DSGVO ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; Den Verantwortlichen trifft die Rechenschaftspflicht der DSGVO und damit alle datenschutzrechtlichen Verantwortlichkeiten wie insbesondere die Sicherstellung der rechtlichen Zulässigkeit von Datenverwendungen, die Vorkehrung von Datensicherheitsmaßnahmen, die Wahrung von Datengeheimnissen, Informationspflichten gegenüber Betroffenen, Auskunftspflichten gegenüber Betroffenen über die zu ihrer Person verarbeiteten Daten, bestimmte Richtigstellungs- und Löschungsverpflichtungen, umfangreiche Dokumentationspflichten (Verfahrensverzeichnisse, Datenschutzfolgeabschätzung, andere Dokumentationen) etc.
Auftragsverar-beiter	eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Auftragsverarbeitung liegt also vor, wenn Dritte im Auftrag des Verantwortlichen Daten verarbeiten. Jeglicher potentielle Zugriff auf personenbezogene Daten durch Dritte unterliegt demnach den Regeln einer Auftragsverarbeitung, auch Zugriff über einen remote access durch Dritte fällt darunter.

Wichtige Begriffe.

Verarbeitung	Das ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
Personenbezogene Daten	Das sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden "betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind; Der Begriff ist sehr weit zu verstehen, im Zweifel ist eine Information, die die Identität einer betroffenen Person bestimmt oder diese bestimmbar macht, als personenbezogenes Datum zu qualifizieren.

Wichtige Begriffe.

Betroffene(r)	Betroffene gemäß der DSGVO sind alle identifizierten oder identifizierbaren natürlichen Personen, deren Daten verarbeitet werden.
Verletzung des Schutzes personenbezogener Daten	eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;
Pseudonymisierung	Das ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden; Beim Pseudonymisieren bleibt der Personenbezug erhalten, er wird aber „versteckt“.

Anwendungsbereich

Anwendungsbereiche.

- **Territorialer Anwendungsbereich**
  - Sehr breiter territorialer Anwendungsbereich: nicht nur Unternehmen mit Niederlassung in der EU, sondern es reicht, wenn Güter oder Dienstleistungen, unabhängig einer Bezahlung, Betroffenen im Unionsgebiet angeboten werden oder Verhalten von EU Bürgern innerhalb der EU beobachtet werden;

- **Kinder**
  - **Personen unter 14 Jahren**.
  - Datenschutzrechte Kinder werden besonders streng gehandelt und unterliegen auch strengeren Strafen als andere DS Verletzungen (Kategorie 20 Mio Euro oder 2 % des weltweiten Umsatzes, je nach dem was höher ist)
  - Der VV muss bei Diensten der Informationsgesellschaft beweisen, dass er alles getan hat, die Zustimmung des Elternteils zu bekommen;

Jede Datenverarbeitung, egal welche Technologie.

- Der Schutz gilt bei jeglicher zumindest teilautomatisierten Datenverarbeitung, egal mit welcher Technologie.
- Ausgenommen sind Datenverarbeitungen im **persönlichen und haushaltsbezogenen** Bereich (Adressverwaltung, Social Networking, online Aktivtäten in diesem Zusammenhang)
- Ebenso **ausgenommen sind anonymisierte Daten**, eine Person darf dann aber **nicht mehr identifizierbar** sein (strengere Anforderungen als jetzt!)

Datenverarbeitung – wie geht das jetzt

Grundsatz der Zweckbindung.

Daten dürfen nur für

- **festgelegte,**
- **eindeutige** und
- **legitime**

Zwecke erhoben werden

und

dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;

Grundsätze der Transparenz, Richtigkeit, Integrität, Vertraulichkeit.

- Umfassende Informationspflichten
- Betroffenenrechte
- Pflicht, Daten aktuell und richtig zu halten
- Daten vor unrechtmäßigem Verlust und vor Zerstörung schützen
- Vertraulichkeit ist zu wahren
- Zugang zu Daten nur nach dem „need to know" Prinzip
- Zugang zu Zugriffsregelungen etablieren

Grundsatz der Datenminimierung.

Personenbezogene Daten müssen

- dem Zweck **angemessen** und
- **erheblich** sowie
- auf das für die Zwecke der Verarbeitung **notwendige Maß** beschränkt sein

Das bedeutet

- Immer nur so wenig Daten wie möglich verarbeiten
- Daten immer nur so kurz wie notwendig mit Personenbezug belassen

Grundsatz der Rechenschaftspflicht.

- Umfassende Dokumentationspflichten
- Datenschutz Risikofolgenabschätzung (Privacy Risk Assessment)
- Führung eines Verfahrensverzeichnis
- Einhaltung von Data pivacy by Design und Data Privacy by Default

Privacy by Design und Privacy by Default.

- **Privacy by Design**:
  - Vorgaben der DSGVO sind von Anfang an zu berücksichtigen, bereits im Design einer Anwendung, eines Produkts, Systems etc.
  - Korrektur/Änderung im nachhinein oft gar nicht oder nur sehr schwer/mit zusätzlichen Kosten möglich.
  - Es sind „angemessene technische und organisatorische Maßnahmen. Wie zB Pseudonymisierung-, mit denen die wirksame Umsetzung der Datenschutzgrundsätze erzielt wird, zu treffen

- **Privacy by Default:**
  - Es muss durch Voreinstellungen sichergestellt sein, dass nur solche personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind, verarbeitet werden (gilt für Umfang der Verarbeitung, Speicherfrist, Zugänglichkeit)

Systeme, die nicht DSGVO konform sind, dürfen nicht (mehr) angewendet werden.

Einwilligung.

- Einwilligung ist notwendig, **wenn keine andere Voraussetzung** für die Datenverarbeitung vorliegt

- **Strenge Anforderungen** an eine Einwilligungserklärung eines Betroffenen, aber **Erleichterungen** hinsichtlich der **Form** der Erklärung:

  - geht nicht nur schriftlich, sondern auch elektronisch oder sogar mündlich;
  - Nicht erlaubt sind stillschweigende Zustimmungserklärungen bzw. vorangeklickte Felder;
  - es braucht immer eine aktive Erklärung des Betroffenen. Die Erklärung muss vom sonstigen Text unterscheidbar sein.

Einwilligung.

- Die Einwilligungserklärung muss **einfach zugänglich, verständlich und in einfacher und klarer Sprache formuliert sein und freiwillig abgegeben werden**. Ein Widerruf muss genauso einfach sein.

- Die Einwilligung hat **folgende Informationen** zu enthalten

  - Information über V und Dritte (wenn es einen Auftragsverarbeiter gibt, der auch Zugang zu Daten hat)
  - Kontaktinformationen zum Datenschutzbeauftragten
  - Zweck der Datenverarbeitung
  - Hinweis, dass die Einwilligung jederzeit widerrufen werden kann (inkl. Widerrufsinformationen

Einwilligung.

- Für **jeden Zweck** ist eine eigene Einwilligung notwendig

- Für die Beurteilung der Freiwilligkeit ist mit zu berücksichtigen, ob die Einwilligung für die Nutzung des Dienstes notwendig ist oder nicht. **Nicht zulässig ist eine konditionale Verknüpfung von Datenverarbeitung** mit dem Dienst, wenn es Daten betrifft, die ich dafür eigentlich nicht brauche. Auch berücksichtigt werden muss, ob ein **Ungleichgewicht** besteht zwischen Erklärendem und Erklärungsempfänger (z.B. im Arbeitsverhältnis).

- Durch den **Widerruf** darf der betroffenen Person kein Nachteil für die gebuchte Dienstleistung erwachsen.

- **Dokumentationspflicht**
  Es ist zu dokumentieren, wer, wann und für was eingewilligt hat.
  - Welcher Kunde hat genau eingewilligt (Speicherung von IP-Adresse, Kundendaten, etc.)
  - Genauer Text, dem eingewilligt wurde (Versionen können sich ändern)
  - Auch bei mündlicher Einwilligung erforderlich

Einwilligung.

- Wenn **bei Inkrafttreten** der DSGVO schon eine **Zustimmung** gemäß derzeit geltender DS Richtlinie vorliegt, braucht keine neue Zustimmungserklärung eingeholt werden, sofern die ursprüngliche Zustimmungserklärung halbwegs den Regelungen der neuen DSGVO entspricht

- Bei **Änderungen** im Prozess, der Zwecke oder der Parteien ist eine neue Einwilligung einzuholen

Einwilligung.

- **Sonderbestimmungen** für die Einwilligung von Kindern im Online Kontext: der VV muss zumutbare Maßnahmen ergreifen, um die Zustimmung des Erziehungsberechtigten zu verifizieren.
  - Wird das Kind geschäftsfähig, so hat es selbst noch einmal eine Einwilligung abzugeben

- Die Einwilligung ist in **regelmäßigen Abständen einzuholen**, alle 2 Jahre wird empfohlen;

- **Sonderfall Direktmarketing**:
  - Werden Daten zum Zwecke des Direktmarketing verarbeitet, so wir das per se als rechtmäßig erachtet.
  - Der Betroffene hat aber ein jederzeitiges Widerspruchsrecht, über das er in einer deutlichen Art und Weise und getrennt von den inhaltlichen Informationen aufzuklären ist.

Besondere Kategorien personenbezogener Daten.

Definition (Artikel 9 DSGVO):
Daten, aus denen die rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zu eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person;

- **Die Verarbeitung ist grundsätzlich untersagt!**

- Wenige Ausnahmen vom Verbot wie zB:
  1. Einwilligung der betroffenen Person
  2. Verarbeitung erforderlich für Verantwortliche wegen Pflichten/Rechten aus Arbeitsrecht, Recht der sozialen Sicherheit und des Sozialschutzes
  3. Zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritte, welche aus körperlichen oder rechtlichen gründen nicht einwilligen können
  4. Verarbeitung erfolgt aufgrund geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnabsicht…
  5. Betroffene Person hat Daten offensichtlich öffentlich gemacht
  6. …….

Profiling

Profiling und rein automatisierte Entscheidungsfindung über Personen.

- Entscheidungen insbesondere in Fällen von **Kreditvergabe und im Arbeitsrecht** dürfen nicht ausschließlich auf profiling oder ein online Verhalten des Betroffenen gestützt werden.

- Die MS können hier Ausnahmen vorsehen, insbesondere für Zwecke der Fraudbekämpfung, Steuerfahndung und sonstigen Präventionsmaßnahmen, um die Leistungen des Datenverarbeiters sicherzustellen.

- Zulässig ist es auch, wenn der Betroffene einwilligt, hier gelten aber besonders strenge Anforderungen, denn der Betroffene muss ausführlich darüber informiert werden und er muss das Recht auf menschliche Intervention in einem automatisierten Prozess haben.

- Erlaubt ist es auch, wenn es zur Vertragserfüllung notwendig ist.

- **Nicht erlaubt ist es bei Kindern**.

Betroffene und ihre Rechte

Wer sind (meine) Betroffenen.

- Recht auf Information;
- Recht auf Auskunft
- Recht auf Richtigstellung
- Recht auf Löschung
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Recht auf Vergessenwerden (= Recht auf Löschung)

Informationspflichten.

- **An wen und wann?**
  - Information an Betroffene, wenn
  - Daten erhoben werden,
  - ein Zweck sich ändert,
  - Daten an Dritte weitergegeben werden etc).

- **Wer muss informieren?**
  - Der, der Datenverarbeitung tatsächlich durchführt (kann VV oder AV sein).

- **Wie?**
  - Information an Betroffene muss klar, leicht verständlich transparent, leicht zugänglich in einfacher Sprache sein. Schriftlich oder auch elektronisch, wo es angebracht ist.

  - Die Information kann (insbesondere im online Bereich) auch in Form von Standardicons gegeben werden. Dazu wird es einheitliche Vorgaben der EU Kommission geben.

Informationspflichten.

- **Was?**
  - Umfangreiche Informationspflichten, wenn Daten direkt vom Betroffenen gesammelt werden und wenn Daten von Dritten kommen.
    - ✓Zweck
    - ✓Rechtliches Interesse des Controllers oder einer 3rd Party
    - ✓Gegebenenfalls Empfänger oder Kategorien von Empfängern
    - ✓Wenn der Auftraggeber Daten in ein EU Drittland übermitteln wird
    - ✓Dauer der Datenspeicherung
    - ✓Belehrung über Rechte des Betroffenen zu Richtigstellung und Löschung und der Portabilität
    - ✓Beschwerderecht
    - ✓Basis ist Gesetz oder Vertrag
    - ✓i.a. automatisierte Entscheidungsprozesse inkl. Profiling
    - ✓Bei Zweckänderung
  - Informationspflichten, wenn die Daten nicht direkt vom Betroffenen gesammelt werden
    - ✓s.o. plus Info, von wo die Daten her sind

Recht auf Auskunft.

- Rechtsmittelbelehrung erforderlich
- Beauskunftung binnen 1 Monat (2 Monate) nach Anfrage,
- Wenn Anfrage elektronisch kommt, muss sie auch elektronisch beantwortet werden, außer der Betroffene will was anderes.
- Beauskunftung ist grundsätzlich gratis.
- Neu ist auch: Auf Antrag ist der betroffenen Person eine Kopie der personenbezogenen Daten zur Verfügung stellen (dies kann auch durch Fernzugriff ermöglicht werden; eventuell auch möglich, dem Betroffenen einen link zu schicken, auf dem er die Informationen abrufen kann);
- Recht auf Akteneinsicht

Recht auf Datenmitnahme.

- Nur, wenn Daten einem VV im privaten Bereich zur Verfügung gestellt wurden (nicht durch Behörde oder im öffentlichen Interesse verarbeitet);
- Recht gibt es nur, wenn die Rechtsgrundlage für die Datenverarbeitung eine Einwilligung oder ein Vertrag ist.
- Umfasst das Recht, dass Daten an den Betroffenen selbst oder an einen Dritten in einem strukturierten, gängigen und machinenlesbaren Format übermittelt werden;
- Theoretisch kann also Kunde verlangen, dass ich seine Daten an die A1 für einen Vertragsabschluss dort übermittle. Wie genau das funktionieren soll, wird noch zu klären sein.

Pflichten von Datenverarbeitern

Auftrags(daten)verarbeitung.

- Auftragsverarbeitung liegt vor, wenn **ein Dritter Teil der Datenverarbeitung** ist
- Verantwortlicher hat **Weisungsbefugnis** an Auftragsverarbeiter
- **Vertrag abzuschließen Ist zwingend** (wie auch bisher)
- VV trifft besondere **Sorgfaltspflicht hinsichtlich Auswahl** des Dienstleisters und muss dies auch dokumentieren
- Auftragsverarbeiter unterliegt selbst auch den Strafbestimmungen der DSGVO
- Achtung **Subauftragnehmer**: nur mit Genehmigung des Verantwortlichen; Auftragsverarbeiter haftet für Subauftragnehmer

Data Breach Notification.

- Bei Datensicherheitsverletzung ist **binnen 72 Stunde** die DSB zu informieren;

- **Wann liegt Datensicherheitsverletzung vor:**
  - ✓ Zugriff durch Personen, die kein need to know haben ist möglich
  - ✓ Unerwünschte Veränderung der Daten ist möglich
  - ✓ Verlust von Daten ist möglich
  - ✓ Unbeabsichtigte Zerstörung oder Löschung von Daten

- **Zusätzlich sind Betroffene unverzüglich zu informieren**, sofern die Verletzung voraussichtlich ein **hohes Risiko** für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.

Datensicherheitsmaßnahmen.

- **Pseudonymisierung und Verschlüsselung**
- Sicherstellung von **Geheimhaltung, Integrität, Zugänglichkeit und Resilienz** der Systeme und Services, die personenbez Daten verarbeiten
- Möglichkeit, Daten **wiederherzustellen**, die durch einen physikalischen oder technischen Zwischenfall verloren gegangen sind
- **regelmäßige Tests, Assessment und** Evaluierung der Effektivität der technischen und organisatorischen Maßnahmen, die die Datensicherheit gewährleisten sollen
- geeignete Maßnahmen vorsehen, die sicherstellen, dass jede Person, die Zugang zu Daten hat, **dies nur nach Instruktionen des VV** nutzt.

§ 11 DSG Datengeheimnis iVm § 69 (Verwaltungsstrafe von 50.000,- bei vorsätzlicher Verletzung)

Verarbeitungsverzeichnis.

- **Pflicht zu Selfassessment von Datenverarbeitungssystemen**
- Nicht verpflichtet für Unternehmen/Einrichtungen mit **weniger als 250 Mitarbeiter**
- **Wichtiges Werkzeug**, hilft eine Datenverarbeitung **strukturiert** nach den Anforderungen der DSGVO zu **prüfen**;
- **Elektronischer Workflow** (Nachweisbarkeit, Auditfähigkeit von Genehmigungen, Versionenhistorie, etc.);
- **Review alle 2 Jahre** oder bei inhaltlicher Änderung der Datenverarbeitung;
- Aufbau gemäß DSGVO **inklusive erste Risikoabschätzung/Risikobewertung** (für Entscheidung, ob DSFA notwendig oder nicht);
- Zusätzliche Kriterien machen VVZ zu **nützlicher Checkliste**

Datenschutzfolgeabschätzung.

- Risikofolgeabschätzung **zwingend, wenn Datenverarbeitungen risikobehaftet** sein können, insbesondere wenn neue Verfahren eingeführt werden;
- Die Aufsichtsbehörde **kann Liste mit bestimmten Arten von Prozessen veröffentlichen, die unbedingt einem solchen assessment zu unterziehen sind** bzw. auch eine Liste mit solchen Prozessen, für die das ausdrücklich nicht gilt
- **Systematische Prozessbeschreibung** und Zweck und das rechtliche Interesse des VV an der DVV
- **Prüfung der Notwendigkeit und Verhältnismäßigkeit im Hinblick auf den Zweck**
- Beurteilung der Risiken für die Rechte und Freiheiten des Betroffenen
- Die **Maßnahmen**, die die Risiken adressieren sollen inkl. Sicherheiten
- **Sicherheitsmaßnahmen** und Mechanismen für Datenschutz und Beschreibung wie die DSGVO damit eingehalten wird
- **Vorab Konsultation der DSB, wenn hohes Risiko festgeste**llt wird; DSB hat dann innerhalb von 8 Wochen (plus max weiteren 6 Wochen) Maßnahmen dazu empfehlen;

Datenschutzbeauftragte(r)

Datenschutzbeauftragte(r).

- **(Verpflichtender) Datenschutzbeauftragter**
  - Information und Beratung des Unternehmens und der Mitarbeiter, die personenbezogene Daten verarbeiten entspr. DSGVO
  - Überwachung der Einhaltung der DSGVO inkl. training und audits
  - Kooperation mit und Ansprechpartner für Datenschutzbehörde
  - Muss weisungsfrei arbeiten und direkt dem obersten Management berichten
  - Klare Abgrenzung zwischen DSB und CISO sollte geregelt werden

Siehe auch Rollenbild der österreichischen Datenschutzbeauftragten unter www.privacyofficers.at/Privacyofficers_Rollenbild_v1.0.pdf

Aufgaben Verantwortlicher.

Rechenschaft

- Verfahrensverzeichnis
- Management der Auftragsverarbeiter
- Privacy By Design
- Privacy by Default
- Compliance bei neuen Datenanwendungen
- Durchführung von Datenschutzfolge-abschätzungen (DPIA)

Transparenz

- Etablierung eines Datenschutz-management-systems
- Informationen an Betroffene
- Regeln für Datentransfer in nicht EU Länder

Information

- Beratung und Schulung der Mitarbeiter
- Fortbildungen/ Ausbildungen

Kommunikation

- Zusammenarbeit mit der Aufsichtsbehörde
- Bearbeitung und Beantwortung von Anfragen von Betroffenen
- Bearbeitung und Meldung von Sicherheitsvorfälle

Aufgaben Datenschutzbeauftragte(r).

Kontakt

- Zusammenarbeit mit der Aufsichtsbehörde
- Ansprechpartner für Aufsichtsbehörde

Beratung

- Beratung des Managements
- Beratung der Mitarbeiter
- Beratung der Betroffenen

Training

- Schulung der Mitarbeiter

Kontrolle

- Datenschutzfolge-abschätzung
- Kontrolle der Befolgung der DSGVO
- Kontrolle ob Datenschutz-management-system gelebt wird
- Berichte an oberstes Management

Schulbezogene Fragen

Rechtsgrundlagen

- **DSGVO** gilt unmittelbar

- **Relevante Gesetze**:
  - Schulunterrichtsgesetz
  - Bildungsdokumentationsgesetz

- **Verantwortlicher** ist der Schulleiter bzw. bei Privatschulen der Schulerhalter (§ 2 Bildungsdokumentationsgesetz)

- **Betroffene**: alle natürlichen Personen, deren Daten die Schule verarbeitet: Lehrer, Schüler, Eltern, sonstige Angestellte

Datenverarbeitung in der Schule

- **Daten**: Name, Adresse, Alter Familienstand etc; **aber auch Artikel 9 DSGVO** Daten: Gesundheitsdaten, ev politische Orientierung (Gewerkschaft)

- **Datenweitergabe an Elternverein:** Schule braucht Zustimmung der Eltern, dass sie Daten der Eltern an EV weitergeben darf oder EV holt sich Daten direkt

- **Kommunikation über Social Media**:

Fotos

Sachverhalt	Rechtliche Grundlage
Schulalltag	zustimmungspflichtig: Schüler/Eltern
Schulausflüge	Zustimmungspflichtig mit Widerrufsrecht oder berechtigtes Interesse der Schule mit Widerspruchsrecht?
Schulveranstaltungen intern	Zustimmungspflichtig mit Widerrufsrecht oder berechtigtes Interesse der Schule mit Widerspruchsrecht?
extern	Begleitung in Informationstext mitaufnehmen, Aushang bei der Veranstaltung mit Information sichtbar anbringen
Schulhomepage	zustimmungspflichtig: Schüler/Eltern
Social Media Auftritt der Schule	zustimmungspflichtig: Schüler/Eltern
Fotos durch Dritte (Eltern, Besucher, andere Schüler etc):	wenn für den eigenen haushaltsbezogenen Bereich: Ausnahmebestimmung von Art greift, DSGVO nicht anwendbar

Klassenbuch § 77 SchulUntG

- **Rechtspflicht:** An jeder Schule ist für jede Klasse ein Klassenbuch zu führen.

- **Ziel:** Das Klassenbuch dient dazu, zur Sicherstellung und zum Nachweis der Ordnungsgemäßheit des Unterrichts Vorgänge zu dokumentieren, die im Zusammenhang mit der Organisation und der Durchführung von Unterricht stehen.

- **Daten:** Klassenbücher haben Aufzeichnungen zu enthalten insbesondere über:
  1. Schule, Schulart, Schulstandort, Schuljahr, Klasse bzw. Jahrgang, Schulformkennzahl,
  2. Namen der Schülerinnen und Schüler,
  3. Unterrichtsgegenstände (Stundenplan),
  4. Namen der unterrichtenden Lehrerinnen und Lehrer,
  5. Termine für Schularbeiten und Tests,
  6. Anmerkungen zu den einzelnen Unterrichtsstunden: Beginn und Ende der Unterrichtsstunde, behandelter Lehrstoff, durchgeführte Prüfungen, besondere Vorkommnisse wie zB Abweichungen vom Stundenplan (Stundentausch, Supplierung, Entfall, Schulveranstaltungen ua.),
  7. Anmerkungen zu den einzelnen Schülerinnen oder Schülern: Fernbleiben, Aufgaben und Funktionen, besondere Vorkommnisse ua.

- **Art 9 DSGVO Daten:**
  dürfen nur dann im Klassenbuch vermerkt werden, wenn deren Dokumentation für die Zweckerreichung gemäß Abs. 1 ein erhebliches öffentliches Interesse darstellt.

Klassenbuch § 77 SchulUntG

- **Datensicherheitsbestimmungen** gem Art 32 DSGVO sind anzuwenden. Klassenbücher sind gesichert und vor dem Zugriff anderer Personen als dem an der Schule tätigen Lehr- und Verwaltungspersonal geschützt zu verwahren

- Sie können statt in Schriftform **auch elektronisch geführt** werden,

- **Need to know Prinzip**:

  Abfrageberechtigungen und das Schaffen von Einsichts- oder Zugriffsmöglichkeiten nur für an der Schule tätigen Lehr- und Verwaltungspersonal, Schülerinnen und Schüler sowie Erziehungsberechtigte zulässig. Für Schülerinnen und Schüler sowie für Erziehungsberechtigte darf ein Personenbezug nur hinsichtlich der eigenen Person bzw. des Kindes, auf das sich das Erziehungsrecht bezieht, hergestellt werden

- **Aufbewahrungsfrist:** drei Jahre ab dem Ende des letzten Schuljahres der betreffenden Klasse oder des betreffenden Jahrganges.

- **Löschpflicht**: Nach Ablauf der Aufbewahrungsfrist gemäß Abs. 4 sind physische Aufzeichnungen zu vernichten und elektronisch gespeicherte Aufzeichnungen zu löschen.

Verein Privacyofficers.at

- **aktives Netzwerk** betrieblicher und behördlicher Datenschutzbeauftragter und sonstiger mit dem Thema Datenschutz Betrauter
- Entwicklung, Darstellung sowie Förderung des **Berufsbildes eines Datenschutzbeauftragten**
- **Plattform** zum Informations- und Erfahrungsaustausch
- fachliche Anleitungen und Empfehlungen (**Best Practice**)
- **Entwicklung von Ausbildungsinhalten** und Förderung entsprechender Maßnahmen im privaten und öffentlichen Bereich
- **Kooperation** mit in- und ausländischen Berufsvereinigungen und internationalen Fachorganisationen aus dem Bereich Datenschutz

Alle Infos: ww.privacyofficers.at

Verein Privacyofficers.at

- **Checkliste Umsetzung der DSGVO**

  https://www.privacyofficers.at/Privacyofficers_Checkliste_Umsetzung_DSGVO_v2.0.pdf

- **Rollenbild der österreichischen betrieblichen und behördlichen Datenschutzbeauftragten**

  https://www.privacyofficers.at/Privacyofficers_Rollenbild_v1.0.pdf

Dr. Natalie Ségur-Cabanac
natalie.segur-cabanac@konfliktundloesung.at
www.konfliktundloesung.at
linked in | twitter | Xing