Datenschutz – alles beim Alten nach der DSGVO?

RZA Business Day

RECHTSANWALT

HON. PROF. DR. LEONHARD REIS

3580 Horn

02982 | 2340

office@leonhardreis.at

Datenschutz

- Jede Verwendung von personenbezogenen Daten unterliegt dem Datenschutzrecht. § 1 DSG 2000 garantiert ein **Grundrecht auf Datenschutz**.
- In persönlicher Hinsicht werden derzeit natürliche und juristische Personen geschützt.
- **Datenverarbeitung**: Erheben, Speichern, Löschen, Verknüpfen, Auswerten…
- Das Kernstück des österreichischen Datenschutzrechts ist das **Prinzip des Verbots mit Erlaubnisvorbehalt**. Eine Datenverarbeitung ist grundsätzlich rechtswidrig, es sei denn, es greift ein Rechtfertigungsgrund. Jede Datenanwendung (auch bei Übermittlung an andere Verarbeiter) bedarf aber eines konkreten Zwecks.
- Unterscheidung personenbezogene und sensible personenbezogene Daten
- Datenverarbeitungsregister (DVR – Nummer) / Standardanwendungen
- Eine **Rechtfertigung** kann vor allem durch gesetzliche Erfordernisse oder Zustimmung des Betroffenen erwirkt werden.

Ein paar Begriffe (1)

- **Personenbezogene Daten (Art 4 Z 1)**
- Definitionsgemäß sind „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person **(„betroffene Person“)** beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer 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.
- **Besondere Kategorien personenbezogener Daten („sensible Daten“, Art 9 Abs 1):**
- Das sind personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Ein paar Begriffe (2)

- **Verarbeitung**
- Unter dem Begriff „Verarbeitung“ versteht die DSGVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten 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.

Ein paar Begriffe (3)

- **Einwilligung (Art 4 Z 11)**
- Als „Einwilligung“ der betroffenen Person gilt jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.
- Diese Einwilligung kann schriftlich, elektronisch oder auch mündlich erfolgen, etwa auch durch Anklicken eines Kästchens auf einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder andere Erklärungen oder Verhaltensweisen, die im jeweiligen Kontext eindeutig das Einverständnis der betroffenen Person zur Datenverarbeitung signalisieren. Stillschweigen, bereits vorangekreuzte Kästchen oder Untätigkeit können keine Einwilligung darstellen. Wenn die Verarbeitung mehreren Zwecken dient, ist für jeden Zweck der Verarbeitung eine gesonderte Einwilligung nötig.
- Eine „ausdrückliche“ Einwilligung ist nur bei der Verarbeitung von sensiblen Daten erforderlich.

Ein paar Begriffe (4)

- **Verantwortlicher (Art 4 Z 7) und Auftragsverarbeiter (Art 4 Z 8)**
- „Verantwortlicher“ 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; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche bzw die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.
- Damit löst der Begriff „Verantwortlicher“ den Begriff „Auftraggeber“ nach dem geltenden österreichischem DSG 2000 ab.
- „Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen bearbeitet.
- Dieser Begriff entspricht daher dem „Dienstleister“ nach dem geltenden DSG 2000.

Grundsätze

- **Welche Grundsätze müssen bei der Verwendung von Daten eingehalten werden?**
- Die Daten dürfen nur nach **Treu und Glauben** und auf **rechtmäßige Weise** verwendet werden. Der **Zweck der Datenverwendung** muss festgelegt, eindeutig und rechtmäßig sein; eine Weiterverwendung in einer mit dem Zweck unvereinbaren Weise ist unzulässig. Die Daten müssen für den Zweck **wesentlich** sein und dürfen im Umfang nicht über den Zweck hinausgehen. Sie müssen **sachlich richtig** sein und, soweit notwendig, auf den neuesten Stand gebracht werden und dürfen nicht länger, als es für die **Erreichung des Zweckes** erforderlich ist, gespeichert werden.
- **Unter welchen Voraussetzungen dürfen Daten verarbeitet werden?**
- Die **Grundsätze der Datenverwendung** müssen eingehalten werden (siehe oben).

- Zweck und Inhalt der Datenanwendung müssen von den **gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen** des jeweiligen Auftraggebers gedeckt sein.
  "Gesetzliche Zuständigkeiten“ beziehen sich auf Auftraggeber des öffentlichen

Grundsätze

- **Unter welchen Voraussetzungen dürfen Daten verarbeitet werden?**
- Die **Grundsätze der Datenverwendung** müssen eingehalten werden.
  Zweck und Inhalt der Datenanwendung müssen von den **gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen** des jeweiligen Auftraggebers gedeckt sein.
- Die **schutzwürdigen Geheimhaltungsinteressen der Betroffenen** dürfen nicht verletzt werden.
  Der Eingriff in das Grundrecht auf Datenschutz darf jeweils nur in erforderlichem Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen **(Verhältnismäßigkeitsgrundsatz).**

Grundsätze

- **Schutzwürdige Geheimhaltungsinteressen bei nicht-sensiblen Daten**
  Schutzwürdige Geheimhaltungsinteressen sind bei Verwendung nicht-sensibler Daten dann nicht verletzt, wenn
  - eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht oder
  - der Betroffene der Verwendung seiner Daten zugestimmt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
  - lebenswichtige Interessen des Betroffenen (zB seine medizinische Behandlung) die Verwendung erfordern oder
  - überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern (zB lebenswichtige Interessen eines Dritten; zur Erfüllung einer vertraglichen Verpflichtung erforderlich; Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde).
  - Ein schutzwürdiges Geheimhaltungsinteresse ist insbesondere auch dann nicht verletzt, wenn nur **zulässigerweise veröffentlichte** Daten oder indirekt personenbezogene Daten verwendet werden.

Neuerungen DS-GVO (1)

Die DS-GVO tritt am 25. Mai 2018 in Kraft und bringt va nachstehende **Änderungen**:

- Erweiterte und neue Rechte für **Betroffene** :
  - Recht auf Information über die Datenverarbeitung (+Speicherdauer)
  - Hinweis auf Herausgabe- und Löschungsrecht
  - Datenportabilität
  - Zustimmung der Kunden zur Datennutzung notwendig

- Verpflichtung zur Bestellung eines **Datenschutzbeauftragten** (DSB), wenn
  - die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird
  - zur Kerntätigkeit „regelmäßige und systematische Überwachung“ gehört
  - Kerntätigkeit erfordert Verarbeitung „besonderer Kategorien“ von Daten

- Freiwillig kann DSB bestellt werden, wobei Vorschriften der DS-GVO einzuhalten sind: Weisungsfrei, Ressourcen, Geheimhaltung, kein Interessenskonflikt

Neuerungen DS-GVO (2)

- Informationspflicht bei **Datenmissbrauch**:
  - Verpflichtung, Verstöße unverzüglich zu melden
  - innerhalb von 72 Stunden nach Kenntnis an die Aufsichtsbehörde + Kunden
  - Überwachung des Datenschutzes künftig daher verpflichtend
    (unerlaubte Zugriffe, Datenexport, Zugriffsprotokollierung bis zu CIO notwendig)

- **Verfahrensverzeichnis** statt Datenverarbeitungsregister:
  - gilt für Unternehmen mit mehr als 250 Mitarbeitern
  - und wenn „Verarbeitung nicht nur gelegentlich“ erfolgt
  - daher eigentlich ALLE
  - Anzugeben sind: Zweck der Verarbeitung; Datenkategorien, Betroffene und Empfänger, Übermittlungen in Drittländer, Löschungsfristen, Datensicherheitsmaßnahmen

Neuerungen DS-GVO (3)

• **Datenschutz-Folgenabschätzung:** Die DSGVO bestimmt, dass eine Datenschutz-Folgenabschätzung insbesondere dann zu erfolgen hat, wenn etwa neue Technologien verwendet werden oder aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht.

- –systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen:
- –bei einer umfangreichen Verarbeitung sensibler Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen oder Straftaten,
- –systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche: z.B. mittels Videoüberwachung.

Verzeichnis (1)

- Der **Verantwortliche** hat ein Verzeichnis sämtlicher Verarbeitungstätigkeiten, die in seiner Zuständigkeit liegen, zu führen. Dieses Verzeichnis hat Folgendes zu enthalten:
- Namen und Kontaktdaten des bzw. der Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten,
- Zweck der Datenverarbeitung
  Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (z.B. Kunden und Lieferanten; Rechnungsdaten, Adressdaten),
- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden (z.B. Sozialversicherung, Finanzamt, Rechtsanwalt, Steuerberater), einschließlich Empfänger in Drittländern oder internationalen Organisationen (z.B. Konzernmutter in USA),
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland (z.B. USA)
- die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien (nach Möglichkeit),
- allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen (nach Möglichkeit).

Verzeichnis (2)

- Über alle im Auftrag eines Verantwortlichen durchgeführten Verarbeitungstätigkeiten hat der **Auftragsverarbeiter** ein Verzeichnis zu führen. Dieses Verzeichnis hat Folgendes zu enthalten:
- Name und Kontaktdaten des Auftragverarbeiters und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragverarbeiters und eines etwaigen Datenschutzbeauftragten,
- Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden,
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder eine internationalen Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation (uU ist auch die Dokumentierung geeigneter Garantien erforderlich).
- allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen (nach Möglichkeit).

Neuerungen DS-GVO (4)

- Erweiterte **Datensicherheitsmaßnahmen** nach dem „Stand der Technik“, zB
  - die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
  - die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
  - die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
  - ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

  Die Einhaltung der Datensicherheit ist nachzuweisen (Datenschutzkonzept).

- Verpflichtung zur Abschätzung der möglichen Folgen einer **Datenverarbeitung**

  Bedrohungen und Schwachstellen für die Rechte und Freiheiten Betroffener sollen vorab identifiziert werden.

Neuerungen DS-GVO (5)

- **Datengeheimnis**
- Diese Bestimmung verpflichtet den Arbeitgeber wie nach bisheriger Rechtslage auch dazu, dass er selbst, sowie seine Dienstleister und Mitarbeiter personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden, geheim zu halten
- Ausdrücklich wird normiert, dass der Arbeitgeber seine Mitarbeiter über die Folgen einer Verletzung des Datengeheimnisses zu belehren hat und dieser vertraglich zu vereinbaren hat, dass das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses einzuhalten ist.

- **Beschwerde an die Datenschutzbehörde**
- Jede betroffene Person hat das Recht auf Beschwerde bei der Datenschutzbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO oder das DSG neu verstößt.
- Der Anspruch auf Behandlung einer Beschwerde erlischt , wenn der Einschreitende sie nicht binnen eines Jahres, nachdem er Kenntnis von dem beschwerenden Ereignis erlangt, längstens aber binnen drei Jahren, nachdem das Ereignis behaupteter Maßen stattgefunden hat, einbringt.
- Die Datenschutzbehörde kann - im Gegensatz zu bisher – bei sämtlichen Verstößen gegen die sogenannten Betroffenenrechte, also beispielsweise gegen das Recht auf Auskunft, das Recht auf Löschung oder das Recht auf Datenübertragbarkeit, mittels Beschwerde angerufen werden

Fit für die DSGVO?

- Bei Nichtbeachtung der DS-GVO drohen dem Unternehmen Geldbußen von bis zu **20 Mio. EUR oder 4 % des weltweiten Konzernjahresumsatzes** (je nachdem, was höher ist)
- Verantwortlich für die Einhaltung der Pflichten der DS-GVO ist das Unternehmen
- Die Bestellung eines DSB ändert an Verantwortung der Geschäftsführung nichts
- Die Maßnahmen der Geschäftsführung sind anhand der „Business Judgement Rule“ zu messen

Analyse

1. Welche Daten werden gespeichert? Welche Daten sind davon personenbezogen?
2. Verfügen sämtliche Bereiche, in denen personenbezogene Daten gesammelt und verarbeitet werden, auch über die entsprechenden Berechtigungen bzw. Zustimmungserklärungen der betroffenen Personen?
3. Stellen wir sicher, dass wir nur notwendige Daten speichern? Und dass wir sie nicht länger als nötig speichern?
4. Wie stellen wir sicher, dass Daten, die wir für einen spezifischen Zweck gespeichert haben, nicht für andere Zwecke genutzt werden?
5. Haben wir die notwendigen Prozesse, um im Falle eines Datenschutzverstoßes die betroffenen Personen und die Aufsichtsbehörden innerhalb von 72 Stunden zu informieren?
6. Können wir rasch feststellen, welcher Mitarbeiter Zugriff auf welche Daten hat?
7. Haben wir einen Prozess, um Betroffenen Auskunft über ihre personenbezogenen Daten zu geben?

Analyse

8. Haben wir die gespeicherten personenbezogenen Daten ausreichend gegen Missbrauch geschützt?
9. Haben wir einen Prozess, um personenbezogene Daten auf Anforderung zu löschen?
10. Wissen wir, welche personenbezogene Daten wir trotz Aufforderung zur Löschung aufbewahren können bzw. auf Grund gesetzlicher Verpflichtungen aufbewahren müssen?
11. Versenden wir sensible personenbezogene Daten unverschlüsselt per E-Mail? Falls ja: wie können wir unsere Kommunikation sicherer machen?
12. Wie gehen wir mit Datentransfers im eigenen Unternehmen um?
13. Wie gehen wir mit grenzüberschreitenden Datentransfers um?
14. Speichern wir personenbezogene Daten im Auftrag anderer Organisationen? Falls ja: halten wir die damit verbundenen Verpflichtungen ein?

Analyse

15. Lassen wir andere Organisationen unsere Daten speichern bzw. übermitteln wir anderen Organisationen Daten? Falls ja: halten wir die damit verbundenen Verpflichtungen ein und verfügen wir über die entsprechenden Zustimmungserklärungen?
16. Brauchen wir einen Datenschutzbeauftragten?
17. Planen wir Schulungen der Mitarbeiter?
18. Sind Änderungen der Verträge mit den Kunden/Nutzern/Subunternehmern notwendig?
19. Ist ein Management für Datensicherheit oder Informationssicherheit vorhanden ?
20. Werden Dokumentationen und Nachweise geführt?
21. Nachweis der Einhaltung der Datensicherheit vorhanden?
22. Wissen wir, wie teuer die Nicht-Einhaltung der EU-Datenschutz-Grundverordnung für uns werden kann?
23. Macht eine entsprechende ISO-Zertifizierung Sinn?

Umsetzung

- Erhebung des Status quo im Unternehmen
- Schulung des neuen Rechtsrahmens für Geschäftsführung/Mitarbeiter
- Prüfung, ob die Bestellung eines DSB für das Unternehmen verpflichtend ist
- Aufbau einer Datenschutzorganisation im Unternehmen
- Erstellung von Verfahrensverzeichnissen
  (= Beschreibungen von Datenanwendungen und der dort verwendeten Datenarten)
- Überprüfung der Datensicherheitsmaßnahmen des Unternehmens aus rechtlicher Sicht

Umsetzung

Nach der DS-GVO hat der DSB bei der Erfüllung seiner Aufgaben im Unternehmen weisungsfrei gestellt zu sein. Ein Unternehmen kann entweder einen externen oder einen internen DSB bestellen.

Meine Kanzlei übernimmt als externer DSB alle gesetzlichen Aufgaben des DSB, zB:

- Laufende Schulung und Beratung der Mitarbeiter des Unternehmens
- Überwachung der Einhaltung der DS-GVO durch das Unternehmen
- Beratung bei der Datenschutz-Folgenabschätzung
- Ansprechpartner der Datenschutzbehörde
- Abschluss von Dienstleisterverträgen

Alternativ kann ein Unternehmen einen internen DSB (Mitarbeiter) bestellen. In diesem Fall unterstützt meine Kanzlei den internen DSB bei der Erfüllung seiner Aufgaben.

Datenschutz – nicht alles beim Alten nach der DSGVO aber auch kein Grund zur Sorge…

DANKE FÜR DIE AUFMERKSAMKEIT!

RECHTSANWALT

HON. PROF. DR. LEONHARD REIS

3580 Horn

02982 | 2340

office@leonhardreis.at