Datenschutzbestimmungen nach DSG 2000

1. Einleitung

Jede Person hat - vor allem in Bezug auf die Achtung ihres Privat- und Familienlebens - Anspruch auf Geheimhaltung der sie betreffenden personenbezogenen Daten, etwa E-Mail, Anschrift, Geburtsdatum oder Telefonnummer. Bei juristischen Personen und Personengemeinschaften (z.B. Verein, GmbH, AG) fallen darunter auch Betriebsgeheimnisse sowie Daten aus dem Geschäftsleben, dem Kunden- und Lieferantenverkehr.

Das Datenschutzgesetz 2000 (DSG) bezweckt den Schutz vor einer raschen, oft unüberlegten Weitergabe von Daten, die von Betroffenen oft nicht gewollt wird, aber nicht mehr in ihrem Einflussbereich liegt. Gerade die neuen Kommunikationsmedien bergen dabei große Gefahren in Sachen Datenmissbrauch.

Zur Sicherung der korrekten Datenverwendung sind Maßnahmen zu treffen, die gegen unberechtigte Speicherung, Veränderung und unrechtmäßige Weitergabe der Daten, aber auch Aktualisierung, Löschung oder Anonymisierung vorgehen.

Um dem entgegen zu wirken, ist - je nach der Art der verwendeten Daten und je nach Umfang und Zweck der Verwendung, unter Bedachtnahme des Stands der technischen Möglichkeiten und der wirtschaftlichen Vertretbarkeit - sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung / vor Verlust geschützt sind und die Verwendung ordnungsgemäß erfolgt.

1.1. Arten von Daten

Personenbezogene Daten: Als „personenbezogene Daten“ versteht man Daten, durch die Betroffene identifizierbar oder bestimmbar sind.

Indirekt personenbezogene Daten: Als „indirekt personenbezogene Daten“, versteht man Daten, die über rechtlich zulässige Mittel nicht auf die Identität des Betroffenen schließen lassen (z.B. verschlüsselte Daten). Diese Daten sind datenschutzrechtlich privilegiert.

Sensible Daten: Als sensible Daten gelten jene, die auf ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit und Sexualleben schließen lassen. Für eine Verwendung dieser Daten ist eine Vorabkontrolle durch die Datenschutzbehörde vorgesehen und sie ist an strenge Verwendungsvoraussetzungen geknüpft.

1.2. Schutzwürdige Daten

Folgende Daten gilt es zu schützen, wobei die Schutzwürdigkeit und damit die Vermutung der Unzulässigkeit einer Übermittlung von oben nach unten zunehmen.

- Name, Anschrift, Geburtsdatum, Telefonnummer
- Information aus öffentlichen Quellen, berufliche Stellung, Ausbildung
- Finanzielle Stellung, Einkommen, Bonität, finanzielle Verpflichtungen
- Freizeit-, Lebens- und Kaufgewohnheiten, Liebhabereien
- Verdachtsmomente, Vorstrafen, Intimleben, psychisch relevante Daten, Familiendaten
- Ethnische Herkunft, politische Meinung, Gewerkschafszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit, Sexualleben

Personenbezogene Daten sind als schutzwürdig zu erachten, sensible Daten als besonders schutzwürdig. Nicht schutzwürdig sind öffentlich zugängliche Daten wie aus dem Grundbuch, Telefonbuch, einem öffentlichen Register oder Daten, die wegen ihrer mangelnden Rückführbarkeit de facto keine „personenbezogenen Daten“ darstellen.

2. Pflichten der Mitarbeiter_innen

2.1. Wesentliche Maßnahmen

Es ist grundsätzlich untersagt, unbefugten Personen oder unzuständigen Stellen Daten mitzuteilen oder ihnen die Kenntnisnahme zu ermöglichen, sowie Daten zu einem anderen als dem zum jeweiligen rechtmäßigen Aufgabenvollzug gehörenden Zweck zu verwenden.

Daten, die einem aufgrund einer berufsmäßigen Beschäftigung anvertraut oder zugänglich gemacht wurden, sind geheim zu halten - und nur aufgrund einer ausdrücklichen mündlichen oder schriftlichen Anordnung des Sicherheitsbeauftragten oder dessen Stellvertretung weiterzugeben.

Diese Verpflichtung besteht auch nach Beendigung der Tätigkeit und/oder nach dem Ausscheiden aus dem Arbeitsverhältnis fort. Verstöße gegen diese Verpflichtung werden mit einer Verwaltungsstrafe nach § 52 DSG geahndet und können arbeitsrechtliche sowie schadenersatzrechtliche Folgen haben.

2.2. Umgang mit Daten

Daten dürfen nur verwendet werden

- nach Treu und Glauben und auf rechtmäßige Weise
- für festgelegte, eindeutige und rechtmäßige Zwecke
- soweit sie für den Zweck der Datenanwendung wesentlich sind und darüber nicht hinausgehen
- wenn sie in Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und aktuell gehalten sind
- solange sie in personenbezogener Form aufbewahrt werden, die zum angegebenen Zweck notwendig ist
- anonymisiert oder gelöscht werden, sobald sie nicht länger dem Zweck dienen, für den sie erhoben wurden

2.3. Zustimmungspflicht

Zur konkreten Verwendung der Daten muss eine Zustimmung vorliegen, eine abgegebene Willenserklärung, die von Betroffenen ohne Zwang und in Kenntnis der Sachlage abgegeben wird. Diese Zustimmung ist formlos und kann schriftlich oder mündlich abgegeben werden. Dabei stehen Betroffenen besondere Rechte - wie etwa das Auskunfts-, Richtigstellungs- und Löschungsrecht - zu. Eine öffentliche Verfügbarmachung der Daten schließt diese Zustimmung aus.

2.4. Technische Datensicherheitsmaßnahmen

Daten sind vor zufälliger oder unrechtmäßiger Verwendung und Zerstörung ordnungsgemäß zu schützen, wie im Sicherheitshandbuch vorgesehen. Daher dürfen nur vom IT-Dienstleister zertifizierte Geräte für die Verarbeitung der Daten verwendet werden. Die Ablage hat an zugriffsgeschützten, gesicherten Speicherorten zu erfolgen. Für die automatisierte Verarbeitung werden nur Informationen aus der dafür vorgesehenen Datenbank verwendet. Die Einpflege erfolgt via gesichertem Online-Formular. Die ungesicherte Übermittlung von Kontakten (etwa per E-Mail an externe Empfänger) ist auch zwischen befugten Adressaten untersagt. Bedenken sind ausnahmslos und unmittelbar mit der/dem Sicherheitsbeauftragten zu klären.

2.5. Sofortige Meldung von Missbrauch

Wenn bekannt wird, dass personenbezogene Daten „systematisch und schwerwiegend unrechtmäßig verwendet wurden und dem Betroffenen Schaden droht“, müssen Betroffene über die/den Datenschutzbeauftragten unverzüglich informiert werden. Diese_r legt auch die Form fest. Datenmissbrauch kann u.a. bei unbefugtem Datenzugriff oder bei Diebstahl/Verlust von Datenträgern eintreten. Auch bei Verdacht auf Schadsoftware ist eine unverzügliche Meldung erforderlich.

3. Pflichten des Arbeitgebers

3.1. Meldepflicht beim Datenverarbeitungsregister

Nach den Bestimmungen des DSG 2000 hat jeder Auftraggeber vor Aufnahme einer Datenanwendung eine Meldung an das Datenverarbeitungsregister bei der Datenschutzbehörde DVR-Online zu erstatten - dabei betrifft die Meldepflicht nur personenbezogene Daten.

3.2. Verpflichtungen des Auftraggeber

Das DSG verpflichtet Auftraggeber von Datenverarbeitung zu entsprechenden Maßnahmen, die die Datensicherheit in allen ihren Organisationseinheiten gewährleisten sollen. Dazu gehören:

- Ausdrückliche Festlegung der Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen einzelnen Mitarbeitern des Unternehmens
- Die Verwendung von Daten ist an das Vorliegen gültiger Aufträge zu binden
- Jede_r Mitarbeiter_in ist über ihre/seine - nach dem DSG und nach innerorganisatorischen Datenschutzvorschriften, einschließlich der Datensicherheitsvorschriften - bestehenden Pflichten zu belehren
- Die Zutrittsberechtigung zu den Räumen des Auftraggebers ist zu regeln
- Die Zugriffsberechtigung auf Daten und Programme sowie der Schutz der Datenträger vor Unbefugten ist zu regeln
- Die Berechtigung zum Betrieb der Datenverarbeitungsgeräte ist festzulegen und jedes Gerät ist durch Vorkehrungen bei den eingesetzten Maschinen und Programmen gegen unbefugte Inbetriebnahme abzusichern
- Ein Protokoll ist zu führen, damit alle Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können
- Eine Dokumentation über die getroffenen Datensicherungsmaßnahmen ist zu führen

3.3. Bedingungen für Outsourcing

Ist es notwendig, dass Daten außer Haus bearbeitet werden, so sieht das DSG 2000 diese Möglichkeit vor. Dafür, aber auch für andere Formen der Auslagerung von Datenverarbeitungsmaßnahmen, ist eine vertragliche Vereinbarung in schriftlicher Form mit dem Datenverarbeitungsdienstleister notwendig. Eine Überlassung an den Dienstleister ist nur dann zulässig, wenn dieser Gewähr für rechtmäßige und sichere Datenanwendung bietet. Neben der Vergewisserung, dass der Dienstleister die notwendigen Sicherheitsmaßnahmen vorweisen kann, ist dieser verpflichtet, die Daten ausschließlich im Rahmen der Aufträge zu verwenden, weitere Dienstleister nur unter Einwilligung des Auftraggebers heranzuziehen und nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, zu retournieren, in dessen Auftrag für ihn aufzubewahren oder zu vernichten.

4. Quellen

[1] „Wirtschaftskammer Österreich," [Online]. Available: https://www.wko.at/Content.Node/Service/Wirtschaftsrecht-und-Gewerberecht/Verwaltungs--und-Verfassungsrecht/Datenschutz/Verarbeitung_von_Daten_und_datenschutzrechtliche_Z.html.

[2] „Bundeskanlzeramt Rechtsinformationssystem," [Online]. Available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597.

[3] „Österreichische Datenschutzbehörde Datenverarbeitungsregister," [Online]. Available: https://www.dsb.gv.at/site/6295/default.aspx.

[4] „Arge Daten Privacy Service," [Online]. Available: http://www.argedaten.at/recht/dsg250c_.htm.

[5] „Rechsinfo," [Online]. Available: http://www.rechtsinfo.com/datenschutzgesetz.html.

[6] D. Jahnel, „internet4jurists.at," [Online]. Available: http://www.internet4jurists.at/literatur/datensicherheit.pdf.

[7] „Bundesministerium für Inneres," [Online]. Available: http://www.bmi.gv.at/cms/BK/praevention_neu/info_material/internet/files/IT_Sicherheitshandbuch.pdf.