Merkblatt

Neues Datenschutzgesetz ab 1. September 2023 – Das Wichtigste für den Umgang durch Gewerbebetriebe

1. Ausgangslage und Überblick

Mit dem neuen Datenschutzgesetz (DSG), das am 25. September 2020 nach intensiver Beratung von National- und Ständerat angenommen worden ist und nach einer verlängerten Umsetzungsfrist am 1. September 2023 in Kraft tritt, nimmt der Druck und der Aufwand zur Datenschutz-Compliance auch für Gewerbebetriebe deutlich zu. Dazu trägt namentlich die zunehmende Sensibilisierung für das Thema Datenschutz bei. Mit der digitalen Entwicklung gewinnen der Persönlichkeitsschutz und die informationelle Selbstbestimmung in weiten Bevölkerungskreisen stetig an Bedeutung.

Der Bundesrat konkretisiert das DSG in der Verordnung über den Datenschutz (Datenschutzverordnung, DSV) und in der Verordnung über Datenschutzzertifizierungen (VDSZ), beide vom 31. August 2022.

Grössere Unternehmen und Betriebe mit EU-Bezug dürften bereits mit Inkrafttreten der europäischen Datenschutzgrundverordnung (DSGVO) den Datenschutz entsprechend ausgebaut haben. Denn die DSGVO beansprucht auch für viele Schweizer Unternehmen Geltung (dazu das Merkblatt vom 16. März 2018). Das neue DSG ist zwar keine vollständige Umsetzung der DSGVO. Allerdings werden viele Regelungen im Grundsatz übernommen, um ein vergleichbares Datenschutzniveau zu erreichen, was den grenzüberschreitenden Datenverkehr erleichtert. Weiter ermöglicht die Revision des DSG auch die Ratifikation der Erweiterung der Europarechtskonvention 108 zum Datenschutz.

Territorial gilt wie bei der DSGVO das Auswirkungsprinzip. Das DSG findet also auch auf alle Sachverhalte Anwendung, die sich im Ausland zutragen, sich aber in der Schweiz auf den Datenschutz auswirken.

Grundsätzlich gilt wie bisher das Prinzip der risikobasierten Anwendung der Normen. Je sensibler Daten oder ein Bearbeitungsvorgang im Hinblick auf die Verletzung der Persönlichkeit der betroffenen Personen ist, desto mehr Vorkehrungen müssen getroffen werden, damit es nicht zur Verletzung kommt. Damit soll der Datenschutz bereits im Planungsstadium digitaler Projekte miteinbezogen werden. Umgekehrt müssen sich Unternehmen (gemäss DSG-Bezeichnung «die Verantwortlichen») bzw. die verantwortlichen Leitungsorgane im Rahmen des Risikomanagements auch die Frage stellen, in welchem Umfang sie bereit sind, Restrisiken *bewusst* einzugehen. Unbestritten ist, dass der Datenschutz – verbunden mit der Informationssicherheit – immer mehr zum strategischen Thema wird, welches auf die Agenda der Geschäftsleitung und des Verwaltungsrats gehört.

Unter den gesetzlichen Datenschutz fallen lediglich Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, sogenannte Personendaten. Neu wird sich der Datenschutz wie in der DSGVO aber auf Daten *natürlicher* Personen beschränken. Der bislang bestehende Schutz für *juristische* Personen entfällt. Damit wird das B2B-Geschäft erleichtert. Juristische Personen bleiben aber durch Art. 28 ZGB (Persönlichkeitsschutz) oder durch Art. 162 StGB (Geschäfts- und Fabrikationsgeheimnis) sowie einschlägige Bestimmungen im Kartellgesetz (KG) und im Gesetz über den unlauteren Wettbewerb (UWG) geschützt. Weiterhin durch das DSG geschützt wären Personendaten von Einzelunternehmen. Auch nicht personenbezogene Geschäftsdaten sollten von Unternehmen angemessen geschützt werden. Datenschutz und Informationssicherheit gehen damit Hand in Hand und sollten schon aus Effizienzgründen gemeinsam angegangen werden.

Zu den *besonders schützenswerten* Personendaten, an deren Bearbeitung gesetzlich höhere Anforderungen gestellt werden (z.B. muss die Einwilligung *ausdrücklich* erfolgen), gehörten bislang die religiö-

sen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre und die Rassenzugehörigkeit, ebenso wie Massnahmen der Sozialhilfe sowie administrative und strafrechtliche Verfolgungen und Sanktionen. Neu hinzu kommen genetische und biometrische Daten. Zudem werden neu besondere rechtliche Folgen bzw. Voraussetzungen nicht mehr an den Tatbestand «Persönlichkeitsprofil» sondern an das «Profiling» bzw. an dasjenige «mit hohem Risiko» geknüpft, das den automatisierten Bearbeitungsprozess (Bewertung von Persönlichkeitsprofilen) adressiert. Angesicht der intensiven parlamentarischen Diskussion, welche dieser Entwicklung beigemessen wurde, fallen die praktischen Änderungen diesbezüglich allerdings marginal aus.

Empfehlenswert in der Praxis sind für Unternehmen – auch wenn nicht durchwegs datenschutzrechtlich zwingend –der Erlass von internen Datenschutzrichtlinien (einfaches Regelset kann genügen), die klare Regelung der Verantwortlichkeiten sowie die Schulung und Sensibilisierung der Mitarbeitenden. Wichtig ist neben der vertraglichen Absicherung (z.B. gegenüber Auftragsbearbeitern) auch, den Datenschutz und die Informationssicherheit angemessen zu dokumentieren, insbesondere um im Fall eines Ereignisses nachweisen zu können, dass der Compliance genüge getan wurde. Selbstredend sind auch die nötigen Prozesse innerhalb des Unternehmens und gegenüber Dritten (Aufsichtsbehörden, betroffene Personen etc.) zu definieren, um bei Bedarf effektiv reagieren zu können.

Nachfolgend werden unter Ziffer 2 die für Gewerbebetriebe wesentlichen Regeln bei der Bearbeitung von Personendaten sowie unter Ziffer 3 die Rechte der betroffenen Personen, welche es zu beachten gilt, näher beschrieben. Unter Ziffer 4 werden für das Risikomanagement drohende Konsequenzen bei Datenschutzverletzungen aufgezeigt. Die Verweise auf Artikel (Art.) und Absatz (Abs.) beziehen sich dabei auf das neue DSG.

2. Welche Regeln haben betroffene Unternehmen bei der Bearbeitung von Personendaten zu berücksichtigen?

Gewerbebetriebe haben bei der Bearbeitung von Personendaten namentlich folgende Regeln zu berücksichtigen. Dabei ist zu beachten, dass das Gesetz von einem umfassenden Begriff der Datenbearbeitung ausgeht, der praktisch jeden Umgang mit Personendaten vom Erfassen bis zum Löschen erfasst:

- **Grundsatz der Rechtmässigkeit:** Personendaten müssen rechtmässig bearbeitet werden (Art. 6 Abs. 1 DSG), d.h. die Bearbeitung ist grundsätzlich zulässig, solange sie nicht in Verletzung einer Rechtsnorm erfolgt.

- **Grundsatz der Transparenz:** Dieser ergibt sich aus dem Grundsatz, dass die Datenbearbeitung nach Treu und Glauben erfolgen muss (Art. 6 Abs. 2 DSG). Datenerhebung und Datenbearbeitung müssen grundsätzlich so erfolgen, dass sie der betroffenen Person bekannt sind. Andernfalls kann die betroffene Person ihre Rechte gar nicht geltend machen.

- **Grundsatz der Verhältnismässigkeit:** Gemäss diesem Grundsatz dürfen nur solche Daten erhoben werden, die für den entsprechenden Zweck *notwendig* und *geeignet* sind (Art. 6 Abs. 2 DSG). Zum Grundsatz der Verhältnismässigkeit gehört auch, dass Daten nur *so lange* gespeichert werden dürfen, wie dies für den Zweck notwendig ist.

- **Grundsatz der Zweckbindung:** Gemäss diesem Grundsatz dürfen Daten nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden und sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist (Art. 6 Abs. 3 DSG). Die Daten sind zu vernichten oder zu anonymisieren, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind (Art. 6 Abs. 4).

- **Grundsatz der Richtigkeit:** Wer Personendaten bearbeitet, hat sich über deren *Richtigkeit* zu vergewissern (Art. 6 Abs. 4 DSG). Er hat alle angemessenen Massnahmen zu treffen, damit die Daten

berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind.

- **Grundsatz der Datensicherheit:** Der Grundsatz verlangt den Schutz der Daten durch *technische* und *organisatorische Massnahmen* (Art. 8 DSG). Diese gewährleisten die verschiedenen Schutzziele *Vertraulichkeit*, *Verfügbarkeit* und *Integrität* der Daten sowie die *Nachvollziehbarkeit* der Datenbearbeitung. Auch hier gilt die Verhältnismässigkeit und die Massnahmen müssen dem Stand der Technik entsprechen. Je sensibler die Daten sind, desto höher sind die Anforderungen an die Datensicherheit. Da der Mensch regelmässig das schwächste Glied bei der Datensicherheit ist, sind neben technischen vor allem auch organisatorische Massnahmen von grosser Bedeutung. Konkrete Massnahmen können sein: Zugriffsbeschränkungen, Datenverschlüsselung, Protokollierung, Backups, sichere Entsorgungstechniken, Zugriffs- und Zutrittskontrollen, Reglemente und Weisungen, Schulung und Sensibilisierung, Verträge zur Datenbearbeitung und Geheimhaltung sowie periodische Kontrollen und Verbesserungen. Der Grundsatz der Datensicherheit wird vom Bundesrat in der DSV (Art. 1-6) weiter konkretisiert.

- **Datenschutz durch Technik (sog. Privacy by Design, Art. 7 Abs. 1 und 2 DSG):** Zur Bearbeitung von Personendaten genutzte Systeme sind von Anfang an so zu gestaltet, dass der Datenschutz eingehalten werden kann. Die technischen und organisatorischen Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt, angemessen sein.

- **Datenschutzfreundliche Voreinstellungen** (sog. Privacy by Default, Art. 7 Abs. 3 DSG): Die Verantwortlichen haben die Standardeinstellung am Gerät bzw. an der Software so zu wählen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt. Diese Regel kommt in der Praxis insbesondere beim Akzept von sog. Cookies im Internet zur Anwendung. Wenn man die Voreinstellungen akzeptiert, dürfen nur die für den Dienst zwingend notwendigen Cookies gesetzt werden. Die betroffene Person kann jedoch in den Einstellungen der Website andere Cookies akzeptieren.

- **Einwilligung und Widerspruch:** Eine Einwilligung der betroffenen Person zur Datenbearbeitung durch ein Unternehmen ist grundsätzlich nicht erforderlich, auch nicht bei besonders schützenswerten Personendaten. Von einer Persönlichkeitsverletzung im Sinn von Art. 30 DSG ist dagegen dann auszugehen, wenn die betroffene Person einer Datenbearbeitung ausdrücklich widerspricht. In diesem Fall kann die Persönlichkeitsverletzung einzig durch eine gesetzliche Grundlage oder durch überwiegende Interessen des Verantwortlichen im Sinn von Art. 31 DSG gerechtfertigt werden (vgl. dazu nachfolgend auch die Regel zur Persönlichkeitsverletzung).

- **Informationspflicht:** Die erweiterte Informationspflicht gemäss Art. 19 ff. DSG ist ein wichtiger Aspekt im Rahmen des Grundsatzes der Transparenz. Die betroffene Person soll wissen, welche mit ihrer Person verbundenen Daten zu welchem Zweck erhoben und bearbeitet werden. Grundsätzlich muss dies *vor* der Beschaffung der Daten erfolgen. Werden die Daten nicht direkt bei der betroffenen Person beschafft, erfolgt die Information innert eines Monats nach Erhalt. Gemäss Art. 13 DSV muss die Information in präziser, transparenter, verständlicher und leicht zugänglicher Form erfolgen. Soweit keine gesetzlich begründete Ausnahme vorliegt, gilt eine Informationspflicht bei jeder planmässigen Beschaffung von Personendaten. Ausgenommen von der Informationspflicht sind Personendaten, die nur nebenbei oder zufällig erfasst werden. Ebenfalls nicht dazu gehören ungewollte oder zufällige Datenbeschaffungen.

  Bestandkunden müssen bei Inkrafttreten des neuen DSG nicht informiert werden. Nicht informiert werden muss eine betroffene Person zudem über das, was sie schon weiss. Personen gelten als vorinformiert, wenn sie ihre Personendaten dem Verantwortlichen ohne dessen Zutun zugänglich

machen. Ebenso muss über spätere Änderungen nicht informiert werden. Lediglich wenn der Zweck der Datenverwendung ändert, muss informiert werden. Inhaltlich sind Identität und Kontaktdaten des Verantwortlichen, der Bearbeitungszweck und gegebenenfalls die Empfänger, denen die Daten bekanntgegeben werden, mitzuteilen. Erfolgt eine Bekanntgabe der Daten ins Ausland, sind die entsprechenden Länder anzugeben. Durch verschiedene weitere gesetzliche Einschränkungs- und Ausnahmegründe wird die Informationspflicht beschränkt bzw. aufgehoben, z.B. wenn die Datenbearbeitung gesetzlich vorgesehen ist oder wenn sie im Widerspruch zu überwiegenden Interessen Dritter steht. Kann der Verantwortliche die betroffene Person nur mit unverhältnismässigem Aufwand identifizieren, muss sie bei indirekter Datenbeschaffung nicht informiert werden. Im konkreten Fall lohnt sich die Konsultation der Ausnahmebestimmungen in Art. 20 DSG. Führen Bearbeitungen zu automatisierten Einzelentscheidungen, haben die Verantwortlichen weiteref Informationspflichten gegenüber der betroffenen Person wahrzunehmen und dieser die ihr zustehenden Anhörungs- und Überprüfungsrechte zu gewähren (Art. 21 DSG). Unternehmen kommen der Informationspflicht in der Regel mit der Datenschutzerklärung auf der Website bzw. in AGB nach. Formvorschriften gibt es aber nicht. Unklarheiten werden zugunsten der betroffenen Person bzw. des Kunden ausgelegt und zu Lasten des Verantwortlichen bzw. des Verfassers. Die DSGVO (Art. 12 ff.) enthält Informationspflichten, die über diejenigen im DSG hinausgehen und detaillierter geregelt sind.

- **Bearbeitung durch Auftragsbearbeiter:** Auftragsbearbeitung bedeutet, dass ein Verantwortlicher die Durchführung einer eigenen Datenbearbeitung von einem Dritten (Auftragsbearbeiter) in seinem Auftrag durchführen lässt. Der Verantwortliche hat dabei gegenüber dem Auftragsbearbeiter namentlich die Zweckbindung und die Datensicherheit vertraglich sicherzustellen (Art. 9 DSG). Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen. Diese kann allgemeiner oder spezifischer Natur sein (dazu auch Art. 7 DSV). Kein Vertrag ist erforderlich, wenn ein Gesetz die Auftragsbearbeitung vorsieht. Auch in diesem Fall ist aber die Zweckbindung und die Datensicherheit sicherzustellen.

- **Datenbekanntgabe ins Ausland:** Nach Art. 16 ff. DSG dürfen Personendaten nur dann an einen Empfänger im Ausland bekannt gegeben werden (auch mittels Zugriff auf einen Server in der Schweiz), wenn das Datenschutzniveau im entsprechenden Land ähnlich hoch ist, wie in der Schweiz. Der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) – nach Inkrafttreten des neuen DSG der Bundesrat – führt dafür eine Liste der Staaten, die aus schweizerischer Sicht ein genügendes Datenschutzniveau aufweisen. Verfügt ein Drittstaat über kein gleichwertiges Datenschutzniveau wie die Schweiz, ist die Bekanntgabe dennoch zulässig, wenn der Verantwortliche mit dem ausländischen Datenempfänger die Einhaltung des Schweizer Datenschutzstandards vertraglich regelt. Die in der Praxis am häufigsten verwendeten Vereinbarungen sind die Standardklauseln der Europäischen Kommission, die es für Auftragsbearbeiter wie auch für Verantwortliche als Empfänger gibt. Auch der EDÖB genehmigt und veröffentlicht solche Klauseln. Der Bundesrat konkretisiert die Datenbekanntgabe ins Ausland weiter in der DSV (Art. 8-12).

- **Verzeichnis der Bearbeitungstätigkeiten:** Verantwortliche und Auftragsbearbeiter von grösseren Unternehmen müssen je ein Verzeichnis sämtlicher Datenbearbeitungen führen (Art. 12 DSG). Ausgenommen sind Unternehmen mit weniger als 250 Mitarbeitenden, es sei denn sie bearbeiten in grossem Umfang besonders schützenswerte Personendaten oder sie führen ein Profiling durch (Art. 24 DSV). Für jede Bearbeitungstätigkeit müssen die gesetzlich vorgesehenen Angaben verzeichnet werden. Es sind dies: Identität des Verantwortlichen bzw. des Auftragsbearbeiters, Bearbeitungszweck, Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten, Kategorien der Empfängerinnen und Empfänger, Aufbewahrungsdauer oder Kriterien zu deren Festlegung, wenn möglich Beschreibung der Massnahmen zur Datensicherheit sowie allfällige Zielstaaten, sollten die Daten ins Ausland gehen. Das Verzeichnis sollte stets aktuell sein und einen Überblick über die datenschutzrelevanten Aktivitäten im Unternehmen verschaffen. Da dies für jeden Datenschutz grundlegend ist, lohnt es sich somit auch für kleinere Unternehmen, ein entsprechendes Verzeichnis zu führen, auch wenn diese die gesetzliche Pflicht nicht trifft. Eine Form-

vorschrift gibt es nicht, womit einfache Word- oder Excel-Dokumente genügen. Verzeichnisse, welche gegebenenfalls in Umsetzung der DSGVO erstellt worden sind, können übernommen werden. Neu gibt es für Unternehmen keine Registrierungspflicht von Datensammlungen mehr, wie das im bisherigen DSG geregelt war, aber in der Praxis kaum gelebt worden ist.

- **Datenschutz-Folgeabschätzung (DSFA):** Birgt eine geplante Datenschutzbearbeitung ein hohes Risiko für die Persönlichkeit und die Grundrechte betroffener Personen, muss der Verantwortliche vorgängig eine DSFA machen (Art. 22 DSG). Das hohe Risiko ergibt sich aus den Technologien und der Art bzw. den Umständen der Datenbearbeitungen (Profiling mit hohem Risiko, Bearbeitung besonders schützenswerter Daten). Dabei steht nicht die mögliche Persönlichkeitsverletzung im Fokus, sondern es wird beurteilt, welche Folgen bei welcher Eintretenswahrscheinlichkeit die Datenbearbeitung für die betroffenen Personen haben bzw. wie diese verhindert werden können. Heikel ist eine Datenbearbeitung namentlich dann, wenn es um systematische Überwachungen oder die Bearbeitung von vertraulichen, persönlichen Daten geht, oder es sich um automatisierte Entscheidungen handelt, die durch Nutzung von Technik einen Vertragsabschluss beeinflussen können. Der Verantwortliche muss die DSFA nach Beendigung der Datenbearbeitung mindestens zwei Jahre aufbewahren (Art. 14 DSV). Bleibt nach der DSFA ein hohes Risiko, ist beim EDÖB eine Stellungnahme einzuholen. Dieser kann Einwände anbringen und Massnahmen vorschlagen (Art. 23 DSG). Der EDÖB kann eine DSFA auch einfordern. Liegt ein Zertifikat oder ein Verhaltenskodex vor oder ist ein Datenschutzberater eingesetzt (dazu nachfolgend mehr), kann auf eine DSFA verzichtet werden. Gerade mit Blick auf das Prinzip Privacy by Design (Datenschutz durch Technik) lohnt es sich praktisch in jedem digitalen Projekt, mindesten eine «kleine» DSFA zu machen.

- **Datenschutzberater:** Unternehmen können freiwillig einen Datenschutzberater ernennen (Art. 10 DSG). Dieser kann, muss aber nicht zwingend in einem Arbeitsvertragsverhältnis zum Verantwortlichen stehen. Neben der allgemeinen Beratung und Schulung prüft der Datenschutzberater Datenbearbeitungsvorhaben, die trotz erfolgter DSFA und der Festlegung von Massnahmen noch ein «hohes Risiko» aufweisen. Wird die Prüfung durch den Datenschutzberater vorgenommen, muss der EDÖB nicht mehr konsultiert werden. Dabei muss der Datenschutzberater über entsprechende Fachkenntnisse verfügen. Gleichzeitig sollte er nicht selbst in die Bearbeitung der fraglichen Personendaten einbezogen sein, damit er seine erforderliche Unabhängigkeit, welche in Art. 23 DSV weiter konkretisiert wird, bewahren kann. Gerade für kleinere Unternehmen ist fraglich, ob diese strengen Anforderungen durch den (einzigen) «Vorteil», den EDÖB nicht konsultieren zu müssen, zu rechtfertigen sind. Die Verantwortlichkeiten bei Datenschutz und Informationssicherheit können bzw. müssen in jedem Unternehmen unabhängig von der Einsetzung eines Datenschutzberaters im Sinn von Art. 10 DSG geregelt werden.

- **Verhaltenskodex:** Berufs-, Branchen- und Wirtschaftsverbände können eigene Verhaltenskodizes entwickeln und diese dem EDÖB unterbreiten (Art. 11 DSG). Eine Pflicht zur Unterbreitung besteht nicht, wird jedoch ein Kodex unterbreitet, muss der EDÖB Stellung nehmen. Die Stellungnahmen des EDÖB werden publiziert. Verhaltenskodizes regeln für die Verbandsmitglieder Aspekte des Datenschutzes. Liegt ein solcher Verhaltenskodex vor, entfällt die Pflicht zur DSFA in Bezug auf diese Aspekte (Art. 22 Abs. 5 DSG). Voraussetzung ist, dass der Verhaltenskodex auf einer DSFA beruht.

- **Zertifizierung:** Auch wenn ein Verantwortlicher ein Datenbearbeitungssystem oder -programm einsetzt, das entsprechend zertifiziert ist (Art. 13 DSG), entfällt für dieses die Pflicht zur DSFA (Art. 22 Abs. 5 DSG). Die Zertifizierung ist ein Ausdruck einer gewissen «Angemessenheit», bedeutet aber nicht, dass es später nicht zu Verletzungen des Datenschutzes oder der Datensicherheit kommen kann.

- **Persönlichkeitsverletzung und Rechtfertigungsgründe:** Wer Personendaten bearbeitet, darf die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen (Art 30 DSG). Eine Persönlichkeitsverletzung liegt insbesondere (aber nicht nur) vor, wenn (a) gegen die Grundsätze der Da-

tenbearbeitung gemäss Art. 6 und 8 DSG verstossen wird, (b) Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden oder (c) Dritten besonders schützenswerte Personendaten bekanntgegeben werden.

Eine Persönlichkeitsverletzung ist nicht widerrechtlich, sondern zulässig bzw. «heilt», wenn einer der folgenden Rechtfertigungsgründe vorliegt (Art. 31 Abs. 1 DSG): (a) Einwilligung der betroffenen Person, (b) überwiegendes privates oder öffentliches Interesse oder (c) gesetzliche Grundlage.

Ein wichtiger Rechtfertigungsgrund für Unternehmen ist in der Praxis neben der Einwilligung das überwiegende private Interesse. Dieses wird im Gesetz weiter konkretisiert. Art. 31 Abs. 2 DSG enthält einen nicht abschliessenden Katalog von möglichen überwiegenden Interessen des Verantwortlichen in folgenden Kontexten: (a) Abwicklung eines Vertragsverhältnisses, (b) zwischen Personen in wirtschaftlichem Wettbewerb, (c) Prüfung Kreditwürdigkeit, (d) Veröffentlichung in Medien, (e) Personen des öffentlichen Lebens sowie (f) Forschung, Planung und Statistik.

Dabei werden die Voraussetzungen für eine Rechtfertigung pro Kontext weiter konkretisiert. Ein häufig angerufener Rechtfertigungsfall ist die Prüfung der Kreditwürdigkeit. Das Datenschutzgesetz macht dabei vier Einschränkungen: Erstens dürfen nur noch Daten von Volljährigen bearbeitet werden. Die Daten dürfen zweitens nicht älter als zehn Jahre sein. Nach zehn Jahren darf etwa eine Information, dass eine Person Konkurs gemacht hat, nicht mehr bearbeitet werden. Drittens dürfen Kreditwürdigkeitsprüfungen kein Profiling mit hohem Risiko oder besonders schützenswerte Daten zugrunde liegen. Viertens dürfen die Daten über die Kreditwürdigkeit Dritten nur bekannt gegeben werden, wenn diese die Daten für den Abschluss oder die Abwicklung eines Vertrags mit der betroffenen Person benötigen. Ein Ampelsystem betreffend Zahlungskraft darf weiter angewendet werden.

Zu den Rechtsansprüchen, welche für eine betroffene Person aus einer ungerechtfertigten Persönlichkeitsverletzung resultieren, mehr unter Ziffer 3.

- **Meldepflicht bei Verletzung der Datensicherheit:** Verletzungen der Daten*sicherheit* (z.B. Offenlegung für Unbefugte, Datenverlust, Cyberangriff etc.), die für die Betroffenen zu einem hohen Risiko für ihre Persönlichkeit oder ihre Grundrechte führen, müssen vom Verantwortlichen dem EDÖB «so rasch als möglich» (im Sinn zeitnah) gemeldet werden (Art. 24 DSG). Keine Verletzung der Daten*sicherheit* ist etwa das zu lange Aufbewahren von Daten (Grundsatz der Verhältnismässigkeit bzw. der Zweckbindung), obschon es sich um eine Verletzung des Daten*schutzes* handelt. Eine Meldung ist etwa erforderlich, wenn unverschlüsselte Mitarbeiterdaten (Personaldossier mit Qualifikationen und Lohnangaben) verloren gehen. Das Risiko, dass die Betroffenen beeinträchtigt werden könnten, ist hoch. Kommen verschlüsselte Mitarbeiterdaten abhanden, ist die Sachlage anders zu beurteilen. Meldepflichtig sind der Sachverhalt, mögliche Folgen und getroffene Massnahmen (z.B. werden betroffene Personen informiert). Die betroffenen Personen sind zu informieren, wenn dies zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt. Die Meldepflicht wird in Art. 15 DSV weiter konkretisiert. Namentlich wird vorgeschrieben, dass die meldepflichtige Verletzung der Datensicherheit zu dokumentieren ist. Die Dokumentation ist während zwei Jahren aufzubewahren.

3. Welche (weiteren) Rechte haben die betroffenen Personen?

Aus den unter Ziffer 2 beschriebenen Regeln und Pflichten der Verantwortlichen ergeben sich naturgemäss auch entsprechende Rechte für die betroffenen Personen. Darüber hinaus enthält das DSG weitere Rechte der betroffenen Personen, welche mit der Revision teilweise noch ausgebaut werden. Es sind dies:

- **Auskunftsrecht:** Das Auskunftsrecht der betroffenen Personen gemäss Art. 25 DSG geht weiter als die Informationspflicht des Verantwortlichen. Die betroffene Person kann mehr erfahren, als der Ver-

antwortliche durch seine Informationspflicht offenbaren muss. Bei der Auskunft geht darum, in Erfahrung zu bringen, ob Personendaten bearbeitet werden und wenn ja, welche, sodass die betroffene Person ihre weiteren Rechte geltend machen kann. Dazu gehören neben den bearbeiteten Personendaten als solche Angaben zur Identität des Verantwortlichen, zum Bearbeitungszweck, zur Aufbewahrungsdauer, zur Datenherkunft und gegebenenfalls Informationen über automatisierte Einzelentscheide und die Empfänger (auch als Kategorien). Ziel ist somit, für eine betroffene Person auf Anfrage eine weitgehende Transparenz bei der Datenbearbeitung zu schaffen. Die Auskunft ist in der Regel kostenlos und innert 30 Tagen zu erteilen. Die Auskunft suchende Person muss sich eindeutig identifizieren. Art. 26 DSG regelt die Einschränkungen des Auskunftsrechts. So müssen etwa querulatorische Gesuche nicht bearbeitet werden. Auch kann ein Gesuch aufgrund überwiegender Interessen Dritter zurückgewiesen werden. Andere Ausnahmen sind vorgesehen, namentlich auch für Medien (Art. 27 DSG). Weitere Regelungen zum Auskunftsrecht finden sich in der DSV (Art. 16-19).

- **Datenportabilität** umfasst neu das Recht auf Datenherausgabe und Datenübertragung (Art. 28 DSG). Betroffene Personen können ihre Daten, die sie einem Verantwortlichen bekannt gegeben haben, in einem gängigen elektronischen Format herausverlangen, wenn die Daten automatisiert bearbeitet werden und die betroffene Person zur Bearbeitung eingewilligt hat oder die Bearbeitung im Rahmen eines entsprechenden Vertrags erfolgt. Unter diesen Voraussetzungen kann auch die Datenübertragung auf einen Dritten verlangt werden, wenn dies keinen unverhältnismässigen Aufwand verursacht. Die Datenportabilität kann aus ähnlichen Gründen wie das Auskunftsrecht eingeschränkt werden (Art. 29 DSG). Weitere Regelung zur Datenportabilität finden sich in der DSV (Art. 20-22).

- **Berichtigungsrecht:** Eine betroffene Person kann nach Art. 32 Abs. 1 DSG verlangen, dass unrichtige Personendaten berichtigt werden; dies dürfte namentlich nach der Ausübung des Auskunftsrechts in Frage kommen. Der Verantwortliche kann die Berichtigung verweigern, wenn eine gesetzliche Vorschrift dies verbietet (z.B. Buchführungs- und Aufbewahrungsvorschriften). Kann weder die Richtigkeit noch die Unrichtigkeit der betreffenden Personendaten festgestellt werden, so kann die betroffene Person verlangen, dass bei den Daten ein Bestreitungsvermerk angebracht wird (Art. 32 Abs. 3 DSG).

- **Recht auf Datenlöschung («Recht auf Vergessen»):** Wie erwähnt liegt eine Persönlichkeitsverletzung gemäss Art. 30 DSG u.a. vor, wenn Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden und keine gesetzliche Grundlage und kein überwiegendes privates Interesse Dritter im Sinn einer Rechtfertigung gemäss Art. 31 DSG besteht. Daraus ergibt sich für die betroffene Person ein beschränktes Recht auf Datenlöschung.

- **Weitere Rechtsansprüche:** Bei ungerechtfertigten Persönlichkeitsverletzungen können die betroffenen Personen weitere zivilrechtliche Ansprüche geltend machen. Es sind dies gemäss Art. 32 Abs. 2 DSG (a) das Verbot einer bestimmten Datenbearbeitung, (b) die Untersagung einer bestimmten Bekanntgabe von Personendaten an Dritte und (c) auch die Löschung oder Vernichtung von Personendaten. Aufgrund des Verweises in Art. 32 Abs. 2 DSG auf das Zivilgesetzbuch bestehen gegebenenfalls folgende weiteren Ansprüche: Die Feststellung, Unterlassung bzw. Beseitigung der Rechtsverletzung sowie die Ansprüche auf Schadenersatz, Genugtuung sowie Herausgabe des Gewinns.

4. Welches sind die Folgen von Datenschutzverletzungen?

- Wie im bisherigen Recht können die Verletzung von datenschutzrechtlichen Pflichten auch im neuen DSG sowohl aufsichtsrechtliche (Art. 49 ff. DSG), als auch strafrechtliche (Art. 60 ff. DSG) sowie zivilrechtliche (Art. 30 ff. DSG) Folgen nach sich ziehen. Während im bisherigen Recht die Verletzung von praktisch keinen gesetzlichen Pflichten strafbewehrt war, wird der strafrechtliche Teil des revi-

dierten DSG stark ausgebaut und die möglichen Strafen sind beträchtlich höher. Auch der aufsichtsrechtliche Teil wird ausgebaut, indem der EDÖB weitergehende Kompetenzen erhält. Demgegenüber bleibt der zivilrechtliche Weg praktisch unverändert.

- Der EDÖB eröffnet von Amtes wegen oder auf Anzeige hin eine Untersuchung, wenn genügend Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte (Art. 49 DSG). Bei geringfügigen Verletzungen kann er von einer Untersuchung absehen (Opportunitätsprinzip). Der EDÖB hat neu auch gegenüber Unternehmen weitreichende Untersuchungsbefugnisse bis hin zu Hausdurchsuchungen und Zeugeneinvernahmen (Art. 50 DSG). Bei Datenschutzverletzungen kann der EDÖB verfügen, dass die Bearbeitung ganz oder teilweise angepasst, unterbrochen oder abgebrochen wird und die Personendaten gelöscht oder vernichtet werden (Art. 51 DSG). Gegen Verfügungen des EDÖB kann Beschwerde beim Bundesverwaltungsgericht erhoben werden. Urteile des Bundesverwaltungsgerichts sind beim Bundesgericht anfechtbar. Vorbehalten sind auch Rechtsmittel im Rahmen der Europäischen Menschenrechtskonvention.

- Im Gegensatz zu den europäischen Datenschutzbehörden kommen dem EDÖB auch nach neuem Recht keine (direkten) *aufsichtsrechtlichen* Sanktionsbefugnisse zu. Die fehlbaren Personen werden durch die kantonalen Strafverfolgungsbehörden sanktioniert. Der EDÖB kann einzig Strafanzeige erstatten und im Verfahren die Rechte einer Privatklägerschaft wahrnehmen (Art. 65 Abs. 2 DSG).

- Im neuen DSG drohen Fehlbaren ein *strafrechtliches* Sanktionssystem mit Bussen bis zu CHF 250’000 (Art. 60 ff. DSG). Strafbar sind einzig *vorsätzliches* Handeln und Unterlassen, nicht jedoch Fahrlässigkeit. Nur auf Antrag einer betroffenen Person bestraft werden die Missachtung von Informations-, Auskunfts- und Meldepflichten sowie die Verletzung der beruflichen Schweigepflicht und von Sorgfaltspflichten im Zusammenhang mit der Datensicherheit, der Datenbekanntgabe ins Ausland und der Auftragsbearbeitung. Von Amtes wegen verfolgt wird hingegen die Missachtung von Verfügungen des EDÖB (indirekte Sanktionsbefugnis). Dieser kann ebenfalls Anzeige erstatten, ein Strafantragsrecht hat er hingegen nicht. Zuständig für die Durchsetzung der Strafe sind die kantonalen Behörden mit den herkömmlichen Rechtsmittelwegen. Gebüsst werden grundsätzlich die verantwortlichen *natürlichen* Personen. Dies dürfte in erster Linie die verantwortlichen Mitglieder der Entscheidungsorgane wie Geschäftsleitung und Verwaltungsrat insbesondere im Rahmen ihrer strategischen Organisationspflicht treffen, aber auch die einzelnen Mitarbeiter im Rahmen ihrer operativen Tätigkeiten. Neu kann das Unternehmen selbst bis zu CHF 50’000 gebüsst werden, wenn die Ermittlung der strafbaren natürlichen Person innerhalb des Unternehmens oder der Organisation einen unverhältnismässigen Untersuchungsaufwand mit sich ziehen würde.

  Anders als beim DSG richten sich die Sanktionen nach der DSGVO ausschliesslich gegen *juristische* Personen. Die Datenschutzbehörden in der EU können gegen fehlbare Unternehmen Bussen bis zu 20 Millionen Euro resp. 4 Prozent des weltweit erzielten Jahresumsatzes aussprechen.

- Für die Durchsetzung von zivilen Ansprüchen aus Persönlichkeitsverletzungen gemäss Art. 32 DSG müssen die betroffenen Personen den Weg der Zivilgerichtsbarkeit beschreiten.

- Nicht unerwähnt bleiben dürfen im Zusammenhang mit Datenschutzverletzungen auch Reputations- und Vertrauensrisiken, welche die aufsichts- und strafrechtlichen Risiken um ein Vielfaches übersteigen können. Im Zusammenhang mit Ereignissen zum Datenschutz und zur Informationssicherheit stellen sich für Unternehmen bisweilen gar Existenzrisiken (Business Continuity, Haftung etc.). Dem gilt es im Rahmen des Risikomanagements gebührend Rechnung zu tragen.

5. Disclaimer

Dieses Faktenblatt hat ausschliesslich informativen Zweck und ist weder eine vollständige Checkliste noch kann es eine Rechtsberatung ersetzen. Der Schweizerische Gewerbeverband sgv lehnt jede Haftung ab, die sich im Zusammenhang mit der Anwendung oder der Unterlassung einer Handlung durch

dieses Faktenblatt ergeben kann. Zudem empfehlen wir, sich an die zuständige Branchenorganisation zu wenden, die weitere Hinweise vermitteln kann.

6. Anhang: Musterdokumente

- Datenschutzerklärung (Website)
- Datenschutzrichtlinie (intern)
- Datenbearbeitungsverzeichnis (Struktur)
- Datenschutzfolgeabschätzung (Struktur)
- Auftragsbearbeitungsvertrag
- Datenschutzklausel AGB

Stand: 6. Dezember 2022

Dossierverantwortlicher

Dieter Kläy, Ressortleiter
Tel. 031 380 14 45, E-Mail d.klaey@sgv-usam.ch