Dachorganisation der Schweizer KMU
Organisation faîtière des PME suisses
Organizzazione mantello delle PMI svizzere
Umbrella organization of Swiss SME

An die Mitgliedorganisationen des sgv

Bern, 22. Dezember 2022 sgv-Kl/ye

Zirkular Nr. 2-141 / 2022
Datenschutzgesetz (DSG) und Datenschutzverordnung (DSV): Merkblatt und Mustertexte für die Anwendung in Firmen und Organisationen

Sehr geehrte Damen und Herren

Mit dem neuen Datenschutzgesetz (DSG), das am 1. September 2023 in Kraft tritt, nimmt der Aufwand zur Datenschutz-Compliance auch für Gewerbebetriebe 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.

Das DSG wird in der Verordnung über den Datenschutz (Datenschutzverordnung, DSV) und in der Verordnung über Datenschutzzertifizierungen (VDSZ) konkretisiert.

Mit dem beiliegenden Merkblatt wollen wir Sie informieren und Ihnen mittels Mustertexten Hilfen für die Umsetzung des neuen Datenschutzrechts in Ihren Organisationen bzw. Unternehmen geben.

Für Auskünfte steht Ihnen gerne Dieter Kläy, 031 380 14 45 oder d.klaey@sgv-usam.ch zur Verfügung.

Freundliche Grüsse

Schweizerischer Gewerbeverband sgv

Hans-Ulrich Bigler
Direktor

Dieter Kläy
Ressortleiter

Beilagen
- erwähnt

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

Einleitende Bemerkung:

Die untenstehende Muster-Datenschutzerklärung basiert auf der Annahme, dass nur eine einfache Datenbearbeitung auf der Website stattfindet und keine Daten – insbesondere nicht ins Ausland – weitergegeben werden. Sie genügt also nur in diesen spezifischen Fällen. Falls weitergehende Datenbearbeitungen vorgenommen, weitere Tools (wie etwa Social Media Plugins, Newsletter oder Webanalysetools, z.B. Google Analytics) genutzt oder Daten (ggf. ins Ausland) weitergegeben werden, sollte die Erklärung um entsprechende Hinweise ergänzt werden. Dazu kann der Beizug eines Spezialisten sinnvoll sein.

Namentlich die Angaben in [eckigen Klammern] müssen an die konkrete Situation angepasst werden.

* * * * *

Datenschutzerklärung

Wir schützen Ihre Privatsphäre und Ihre privaten Daten. [Unsere Bearbeitung von Personendaten unserer Nutzer beschränkt sich auf jene Daten, die zur Bereitstellung einer funktionsfähigen Internetseite sowie unserer Inhalte und Leistungen erforderlich sind.] Wir erheben, verarbeiten und nutzen Ihre Personendaten in Übereinstimmung mit dem Inhalt der vorliegenden Datenschutzbestimmungen sowie den anwendbaren Datenschutzvorschriften, insbesondere dem Schweizer Datenschutzgesetz (DSG). In den vorliegenden Datenschutzbestimmungen wird geregelt, welche Personendaten wir über Sie erheben, verarbeiten und nutzen. Wir bitten Sie daher, die nachfolgenden Ausführungen sorgfältig durchzulesen.

1. Verantwortlicher

[Name und Kontaktdaten des Verantwortlichen, ggf. des Vertreters] (Im Folgenden: «**Wir**») ist als Betreiber der Website [Name der Website] Verantwortlicher für die Personendaten der Nutzer (Im Folgenden: «**Sie**») der Website im Sinne des DSG.

2. Beschreibung und Umfang der Datenverarbeitung [ggf. anpassen]

2.1 Personendaten im Sinne dieser Datenschutzbestimmungen sind alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person (im Folgenden „betroffene Person“) beziehen. Hierzu zählen insbesondere Ihr Name, Ihre E-Mail-Adresse [Ihre Adresse und Ihre Telefonnummer sowie Ihre Kreditkarten- und Kontodaten und Ihre Mehrwertsteuerangaben, wenn Sie ein registrierter Händler sind].

2.2 Zu den Personendaten zählen auch Informationen über Ihre Nutzung unserer Website. In diesem Zusammenhang erheben wir Personendaten wie folgt von Ihnen: Informationen über Ihre Besuche unserer Website wie bspw. Umfang des Datentransfers, den Ort, von dem aus Sie Daten von unserer Website abrufen sowie andere Verbindungsdaten und Quellen, die Sie abrufen. Dies geschieht in der Regel durch die Verwendung von Logfiles und Cookies. Nähere Informationen zu Logfiles und Cookies erhalten Sie weiter unten.

2.3 Grundsätzlich werden Ihre Personendaten für die Dauer von [x Wochen/Monaten] gespeichert. Sofern wir Ihre IP-Adresse erheben, wird diese nur für die Zeit Ihrer Nutzung der Website gespeichert und im Anschluss daran unverzüglich gelöscht oder durch Kürzung anonymisiert. Die übrigen Daten werden für eine begrenzte Zeitdauer gespeichert, die sich nach den folgenden Kriterien richtet: [Kriterien].

3. Verwendungszweck [ggf. anpassen]

Wir verwenden Ihre Personendaten zu folgenden Zwecken:

3.1 Um die von Ihnen gewünschten Dienste [ggf. näher spezifizieren, z.B. Warenkorb-Funktionen] zu erbringen;

3.2 Um sicherzustellen, dass unsere Website in möglichst effektiver und interessanter Weise Ihnen gegenüber präsentiert wird [ggf. näher spezifizieren, z.B. Speicherung von Anzeigepräferenzen];

3.3 Um unseren Verpflichtungen aus etwaigen zwischen Ihnen und uns geschlossenen Verträgen nachzukommen [ggf. näher spezifizieren oder löschen];

3.4 Um Ihnen die Teilnahme an interaktiven Angeboten zu ermöglichen, sofern Sie dies wünschen;

3.5 Um Sie über Änderungen unserer Leistungen zu informieren.

3.6 [ggf. weitere Verwendungszwecke]

4. Grundsätze der Datenbearbeitung

Wir berücksichtigen bei der Datenbearbeitung die Bearbeitungsgrundsätze der Rechtmässigkeit, der Verhältnismässigkeit, der Zweckbindung, der Transparenz – insbesondere die Erfüllung der Informationspflichten – und der Datensicherheit.

5. Informationen über Ihren Computer, Cookies [ggf. anpassen]

5.1 Bei jedem Zugriff auf unsere Seite erheben wir folgende Informationen über Ihren Computer: Die IP-Adresse Ihres Computers, die Anfrage Ihres Browsers sowie die Zeit dieser Anfrage. Ausserdem werden der Status und die übertragene Datenmenge im Rahmen dieser Anfrage erfasst. [Wir erheben auch Produkt- und Versionsinformationen über den verwendeten Browser und das Betriebssystem ihres Computers. Wir erfassen weiter, von welcher Website aus der Zugriff auf unsere Seite erfolgte.] Die IP-Adresse Ihres Computers wird dabei nur für die Zeit Ihrer Nutzung der Website gespeichert und im Anschluss daran unverzüglich gelöscht oder durch Kürzung anonymisiert. Wir verwenden diese Daten für den Betrieb unserer Website, insbesondere um Fehler der Website festzustellen und zu beseitigen, um die Auslastung der Website festzustellen und um Anpassungen oder Verbesserungen vorzunehmen.

5.2 Cookies helfen unter vielen Aspekten, Ihren Besuch auf unserer Website einfacher, angenehmer und sinnvoller zu gestalten. Cookies sind Informationsdateien, die Ihr Webbrowser automatisch auf der Festplatte Ihres Computers speichert, wenn Sie unsere Internetseite besuchen.

Wir setzen Cookies beispielsweise ein, um Ihre ausgewählten Leistungen und Eingaben beim Ausfüllen eines Formulars auf der Website temporär zu speichern, damit Sie die Eingabe beim Aufruf einer anderen Unterseite nicht wiederholen müssen. Cookies werden gegebenenfalls auch eingesetzt, um Sie nach der Registrierung auf der Website als registrierten Benutzer identifizieren zu können, ohne dass Sie sich beim Aufruf einer anderen Unterseite erneut einloggen müssen.

Sollten Sie eine Verwendung von Browser-Cookies nicht wünschen, können Sie Ihren Browser so einstellen, dass eine Speicherung von Cookies nicht akzeptiert wird. Bitte beachten Sie, dass Sie unsere Website in diesem Fall allenfalls nur eingeschränkt oder gar nicht nutzen können. Wenn Sie nur unsere

eigenen Cookies, nicht aber die Cookies unserer Dienstleister und Partner akzeptieren wollen, können Sie in Ihrem Browser die Einstellung „Cookies von Drittanbietern blockieren“ wählen.

6. Datensicherheit [ggf. anpassen]

Alle Informationen, die Sie an uns übermitteln, werden auf Servern innerhalb [der Schweiz/Europäischen Union] gespeichert. Leider ist die Übertragung von Informationen über das Internet nicht vollständig sicher, weshalb wir die Sicherheit der über das Internet an unsere Website übermittelten Daten nicht garantieren können. Wir sichern unsere Website und sonstigen Systeme jedoch durch technische und organisatorische Massnahmen gegen Verlust, Zerstörung, Zugriff, Veränderung oder Verbreitung Ihrer Daten durch unbefugte Personen ab. Insbesondere werden Ihre persönlichen Daten bei uns verschlüsselt übertragen. Wir bedienen uns dabei des Codierungssystems SSL (Secure Socket Layer) [bzw. TLS (Transport Layer Security)].

7. Keine Weitergabe Ihrer Personendaten [ggf anpassen]

Wir geben Ihre Personendaten nicht an Dritte weiter, es sei denn, Sie haben in die Datenweitergabe eingewilligt oder wir sind aufgrund gesetzlicher Bestimmungen und/oder behördlicher oder gerichtlicher Anordnungen zu einer Datenweitergabe berechtigt oder verpflichtet. Dabei kann es sich insbesondere um die Auskunftserteilung für Zwecke der Strafverfolgung, zur Gefahrenabwehr oder zur Durchsetzung geistiger Eigentumsrechte handeln.

8. Änderungen dieser Datenschutzbestimmungen

Wir behalten uns das Recht vor, diese Datenschutzbestimmungen jederzeit mit Wirkung für die Zukunft zu ändern. Eine jeweils aktuelle Version ist auf der Website verfügbar. Bitte suchen Sie die Website regelmäßig auf und informieren Sie sich über die geltenden Datenschutzbestimmungen.

9. Ihre Rechte

Sie haben das Recht, Auskunft über Ihre von uns verarbeiteten Personendaten zu verlangen. Insbesondere können Sie Auskunft über die Personendaten als solche, den Bearbeitungszweck, die Aufbewahrungsdauer oder, falls dies nicht möglich ist, die Kriterien zur Festlegung dieser Dauer, die Herkunft Ihrer Daten, sofern diese nicht bei Ihnen erhoben wurden, gegebenenfalls über das Vorliegen einer automatisierten Einzelentscheidung sowie gegebenenfalls über die Empfänger oder die Kategorien von Empfängern, denen Personendaten bekanntgegeben werden verlangen.

Sie haben auch das Recht, eine allenfalls erteilte Einwilligung zur Nutzung Ihrer Personendaten jederzeit zu widerrufen.

Sie können Ihre genannten Rechte jederzeit bei uns geltend machen unter der angegebenen Kontaktadresse.

Sofern Sie der Auffassung sind, dass die Verarbeitung Ihrer Personendaten durch uns im Widerspruch zu den geltenden Datenschutzbestimmungen steht, haben Sie die Möglichkeit, sich beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten zu beschweren.

Stand: [Datum]

Einleitende Bemerkung:

Die untenstehende Muster-Datenschutzrichtlinie fokussiert sich auf das Wesentliche und gibt eine mögliche Struktur vor. Es macht Sinn, diese gemäss Ihrer konkreten Unternehmenssituation zu ergänzen bzw. anzupassen. Dazu kann der Beizug eines Spezialisten sinnvoll sein.

* * * * *

Datenschutzrichtlinie

I. Allgemeines

1. Einleitung

1.1. Die im Unternehmen vorhandenen Datensind für das Unternehmen von grossem Wert. Diese Daten sind daher gegen unbefugte Zugriffe und andere Gefährdungen zu schützen.

1.2 Die Kunden, Partner und Mitarbeiter des Unternehmens erwarten, dass die dem Unternehmen anvertrauten Daten besonders geschützt werden und ein sorgsamer Umgang mit ihnen erfolgt.

1.3 [Bei Fragen zum Thema Datenschutz oder zum Umgang mit Personendaten kann der Datenschutzbeauftragte [Name, Emailadresse/Telefonnummer o.ä.] kontaktiert werden.]

1.4 […]

2. Ziel der Datenschutzrichtlinie

2.1 Mit dieser Datenschutzrichtlinie sollen einheitliche Standards für den Datenschutz im Unternehmen geschaffen werden.

2.2 Durch die Einhaltung der in dieser Datenschutzrichtlinie definierten Standards kommt das Unternehmen seinen datenschutzrechtlichen Verpflichtungen nach und sorgt für eine ausreichende Berücksichtigung der Interessen sowie Rechte der betroffenen Personen.

2.3 Die Beachtung dieser Datenschutzrichtlinie ist Voraussetzung für den sicheren Austausch von Personendaten innerhalb des Unternehmens und mit Dritten.

2.4 […]

3. Anwendungsbereich der Datenschutzrichtlinie

3.1 Diese Datenschutzrichtlinie gilt für jegliche Bearbeitung von Personendaten, wobei insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten erfasst werden. Sie findet Anwendung auf sämtliche Arten von Personendaten, insbesondere Daten von Mitarbeitern, Kunden, Lieferanten und anderen Geschäftspartnern.

3.2 Die Datenschutzrichtlinie beschreibt, konkretisiert bzw. ergänzt dabei auch gesetzliche Vorgaben, namentlich solche aus dem Schweizer Datenschutzgesetz (DSG).

3.3 […]

4. Definitionen

4.1 **Personendaten** im Sinne dieser Unternehmensrichtlinie sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.

4.2 **Betroffene Personen** sind diejenigen natürlichen Personen, über die Personendaten bearbeitet werden.

4.3 **Verantwortlicher** ist eine private Person, die allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet.

4.4 **Auftragsbearbeiter** ist ein Dritter, der im Auftrag des Verantwortlichen Personendaten bearbeitet.

[…]

II. Grundregeln der Datenbearbeitung

5. Rechtmässigkeit

5.1 Personendaten müssen rechtmässig bearbeitet werden. Die Bearbeitung gilt nur als rechtmässig, wenn sie durch (a) Einwilligung der betroffenen Person, durch (b) ein überwiegendes privates oder öffentliches Interesse oder durch (c) Gesetz gerechtfertigt ist.

6. Transparenz

6.1 Die Bearbeitung der Daten muss grundsätzlich so erfolgen, dass sie der betroffenen Person bekannt ist.

7. Verhältnismässigkeit

7.1 Bei der Bearbeitung von Personendaten ist der Grundsatz der Verhältnismässigkeit zu beachten. Gemäss diesem Grundsatz dürfen nur solche Daten erhoben werden, die für den entsprechenden Zweck *notwendig* und *geeignet* sind.

7.2 Weiter dürfen Personendaten nur so lange gespeichert werden, wie dies für den Zweck notwendig ist (vgl. hiernach).

8. Zweckbindung

8.1 Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist.

8.2 Werden die Personendaten zum Zweck der Bearbeitung nicht mehr benötigt, müssen diese vernichtet oder anonymisiert werden.

9. Richtigkeit

9.1 Alle Mitarbeiter haben darauf zu achten, dass Personendaten richtig sind und auf dem neuesten Stand gehalten werden.

9.2 Es müssen alle angemessenen Massnahmen getroffen werden, um unzutreffende oder unvollständige Daten zu berichtigen oder zu vernichten.

10. Datensicherheit

10.1 Für das Unternehmen ist von grosser Bedeutung, dass die Sicherheit der Daten jederzeit gewährleistet ist. Vor diesem Hintergrund sind die Personendaten durch technische und organisatorische Massnahmen u.a. gegen Verlust, gegen unbefugten Zugriff und vor anderen Gefahren zu schützen.

10.2 Für die einzelnen Vorgänge der Datenbearbeitung sind die konkreten Schutzmassnahmen zu dokumentieren und auf ihre Angemessenheit zu überprüfen.

10.3 Die IT-Abteilung kann weitergehende Vorgaben im Interesse der Datensicherheit erlassen, insbesondere in Bezug auf die Nutzung von IT-Systemen im Unternehmen.

11. Einwilligung und Widerspruch

11.1 Eine Einwilligung der betroffenen Person zur Datenbearbeitung durch ein Unternehmen ist grundsätzlich nicht erforderlich, auch nicht bei besonders schützenswerten Personendaten.

11.2 Widerspricht die betroffene Person hingegen einer Datenbearbeitung ausdrücklich, ist diese nur gerechtfertigt, wenn überwiegende Interessen des Verantwortlichen oder eine gesetzliche Grundlage vorliegen.

12. Informationspflicht

12.1 Betroffene Personen müssen möglichst vorgängig informiert werden, zu welchem Zweck Personendaten über sie erhoben und bearbeitet werden. Werden die Daten nicht direkt bei der betroffenen Person beschafft, wird diese innert eines Monats nach Erhalt der Daten informiert.

12.2 Macht die betroffene Person ihre Personendaten dem Verantwortlichen von sich aus zugänglich, gilt diese als informiert.

12.3 Wenn sich der Zweck der Datenbearbeitung ändert, müssen bereits informierte Personen erneut informiert werden.

13. Auftragsbearbeitung

13.1 Wenn Dienstleister des Unternehmens in dessen Auftrag Personendaten verarbeiten (sog. Auftragsbearbeiter), ist zu beachten, dass die gleichen Sorgfaltsanforderungen wie beim verantwortlichen Unternehmen auch für den Auftragsbearbeiter gelten. Insbesondere sind die Zweckbindung und Datensicherheit vertraglich sicherzustellen.

14. Übermittlung von Personendaten ins Ausland

14.1 Die Übermittlung von Personendaten ins Ausland ist nur in Staaten zulässig, in denen durch den Bundesrat ein ähnlich hohes Datenschutzniveau festgestellt wurde, wie in der Schweiz. Eine Einhaltung des Schweizer Datenschutzstandards kann zudem unter anderem durch den Abschluss zusätzlicher vertraglicher Vereinbarungen erreicht werden.

IV. Innerbetriebliche Prozesse

15. Anforderungen an Mitarbeiter

15.1 Alle Mitarbeiter des Unternehmens sind dem Datenschutz verpflichtet. Sie werden namentlich darüber informiert, dass es untersagt ist, Personendaten für private Zwecke zu nutzen, an Unbefugte zu übermitteln oder sie Unbefugten zugänglich zu machen. Die Pflicht zur Wahrung der Vertraulichkeit gilt über das Ende der Anstellung hinaus.

15.2 Auch innerhalb des Unternehmens ist darauf zu achten, dass nur die Mitarbeiter Zugriff auf Personendaten erhalten, die sie zur Erledigung ihrer Aufgaben für das Unternehmen benötigen.

15.3 Alle Mitarbeiter sollen zu Beginn ihrer Anstellung und nachfolgend regelmässig in Datenschutzthemen geschult und sensibilisiert werden.

16. Verzeichnis der Bearbeitungstätigkeiten

16.1 Das Unternehmen führt ein Verzeichnis der Bearbeitungstätigkeiten im Zusammenhang mit Personendaten. Darin müssen festgehalten werden: 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.

17. Datenschutz durch Technik, datenschutzfreundliche Voreinstellungen sowie Datenschutz-Folgeabschätzung

17.1 Zur Bearbeitung von Personendaten genutzte Systeme sind von Anfang an so zu gestalten, 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 (Privacy by Design).

17.2 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. Dies betrifft bspw. den Akzept von Cookies auf der Website.

17.3 Namentlich wenn eine geplante Datenschutzbearbeitung ein hohes Risiko für die Persönlichkeit und die Grundrechte betroffener Personen birgt, ist eine Datenschutz-Folgeabschätzung (DSFA) vorzunehmen und zu dokumentieren.

17.4 […]

V. Rechte der betroffenen Personen

18. Auskunftsrecht

18.1 Auf Anfrage ist einer betroffenen Person mitzuteilen, ob von dem Unternehmen Personendaten über sie bearbeitet werden. Sofern dies der Fall ist, hat die betroffene Person einen

Anspruch auf Auskunft über die entsprechenden Personendaten. Beim Auskunftsrecht geht es 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).

18.2 Bei der Auskunftserteilung ist sicherzustellen, dass die Identität der betroffenen Person verifiziert wird. Weiter ist zu beachten, dass im Rahmen der Auskunftserteilung keine Personendaten Dritter offenbart werden. Die Auskunft ist in der Regel kostenlos und innert 30 Tagen zu erteilen.

19. Datenportabilität / Recht auf Datenherausgabe und Datenübertragung

19.1 Betroffene Personen können ihre Daten, die sie dem Unternehmen 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.

20. Recht auf Berichtigung

20.1 Eine betroffene Person kann nach Art. 32 Abs. 1 DSG verlangen, dass unrichtige Personendaten berichtigt werden.

21. Recht auf Datenlöschung

21.1 Wenn Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden und keine gesetzliche Grundlage und kein überwiegendes privates Interesse Dritter besteht, kann die betroffene Person die Löschung ihrer Personendaten verlangen.

[…]

VI. Zuständigkeit

22. Verantwortung

22.1 In erster Linie sind diejenigen Mitarbeiter für die Einhaltung der Vorgaben dieser Datenschutzrichtlinie verantwortlich, die jeweils mit der Datenbearbeitung betraut sind.

22.2 Alle Mitarbeiter des Unternehmens haben auf die Einhaltung dieser Datenschutzrichtlinie zu achten und auf diese Weise dazu beizutragen, dass in dem gesamten Unternehmen einheitlich hohe Datenschutzstandards etabliert werden.

22.3 Werden gesetzliche datenschutzrechtliche Pflichten verletzt, drohen den Fehlbaren strafrechtliche (Busse bis CHF 250'000.-) und dem Unternehmen zivilrechtliche (bis hin zu Schadenersatz) Konsequenzen sowie Reputationsschäden. Strafrechtlich verantwortlich ist in erster Linie die natürliche Person, d.h. der vorsätzlich fehlbare Mitarbeiter. Datenschutzverletzungen können auch unternehmensinterne disziplinarische Konsequenzen haben.

22.4 […]

23. Meldung von Verstössen und Zusammenarbeit mit Aufsichtsbehörden

23.1 Die Mitarbeiter haben dem Vorgesetzten bzw. dem Datenschutzbeauftragten unverzüglich Bericht zu erstatten, wenn sie Kenntnis von einem Verstoss gegen diese Datenschutzrichtlinie oder gesetzliche Bestimmungen haben, die sich auf den Schutz personenbezogener Daten beziehen.

23.2 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 Unternehmen dem EDÖB «so rasch als möglich», also zeitnah, gemeldet werden.

23.3 […]

VII. Weitere Bestimmungen

24. Publizität

24.1 Diese Unternehmensrichtlinie ist allen Mitarbeitern des Unternehmens in geeigneter Weise zugänglich zu machen, [insbesondere über das Intranet].

24.2 Eine allgemeine Veröffentlichung dieser Datenschutzrichtlinie ist nicht vorgesehen.

25. Änderungen

25.1 Das Unternehmen behält sich das Recht vor, diese Datenschutzrichtlinie bei Bedarf zu ändern. Eine Änderung kann insbesondere erforderlich werden, um gesetzlichen Vorgaben, Forderungen der Aufsichtsbehörden oder unternehmensinternen Verfahren zu entsprechen.

25.2 In regelmässigen Abständen soll auch geprüft werden, inwieweit technologische Veränderungen eine Anpassung dieser Unternehmensrichtlinie erforderlich machen.

26. […]

Spalte	Erläuterung
Datenbearbeitung	Titel / Name der Datenbearbeitung. Bearbeiten ist jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten.
Datenbearbeitungssystem	Name des für die Datenbearbeitung eingesetzten Systems. *Beispiel: CRM*
Bearbeitungszweck	Auflisten aller Zwecke der jeweiligen Bearbeitung, d.h. die Beantwortung der Frage: Für was bearbeiten wir als Unternehmen die Personendaten? *Beispiel: Eintragung eines neuen Kunden in die Kartei.*
Kategorien betroffener Personen	Auflisten aller von der jeweiligen Bearbeitungstätigkeit betroffenen Personen, d.h. die Beantwortung der Frage: Welche Personen werden von der Bearbeitungstätigkeit betroffen indem ihre Personendaten bearbeitet werden? *Beispiel: Kunden, Lieferanten, Personal*

Kategorien bearbeiteter Personendaten	Auflisten aller von der jeweiligen Verarbeitungstätigkeit betroffenen Kategorien der Personendaten, d.h. die Beantwortung der Frage: Welche Personendaten werden verarbeitet? Als Personendaten gelten alle Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. *Beispiel: Name, Vorname, Adresse, Telefonnummer, Emailadresse, IP-Adresse, Zahlungsinformationen usw.*
Empfänger	Auflisten sämtlicher Dritten, an welche die Personendaten weitergegeben werden. *Beispiele: Zahlungsdienstleister, lokale Behörden, Clouddienstleister, Hoster, CRM-Anbieter usw.*
Aufbewahrungsdauer	Dauer der Aufbewahrung der Personendaten oder, falls nicht möglich, die Kriterien zur Festlegung derselben.
Datensicherheit	Sofern möglich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit nach Artikel 8 DSG. *Beispiel: Zugriffsbeschränkungen, Zutrittsbeschränkungen, passwortgeschützte Bereiche, Weitergabekontrolle usw.*
Übermittlung in Drittstaaten	Auflistung aller Drittstaaten, in welchen die Empfänger der Daten ihren Sitz haben bzw. ihre Dienstleistung erbringen (z.B. Standorte der Server) unter Berücksichtigung von Artikel 16 ff. DSG. *Beispiele: USA (Google, Social Media Plattformen etc.), China etc.*

Einleitende Bemerkung:

Das vorliegende Formular gilt als Basis und muss unter Umständen an die konkrete Situation in der entsprechenden Unternehmung angepasst werden. Bei komplexen Abschätzungen empfiehlt sich ein Spezialist beizuziehen.

Formular Datenschutz-Folgenabschätzung

Dieses Formular unterstützt KMU bei der Erstellung einer Datenschutz-Folgenabschätzung (DSFA). Eine DSFA ist zu erstellen, wenn eine neue Bearbeitung von Personendaten beabsichtigt wird und diese ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann.

1 Angaben zum Verantwortlichen

Verantwortlicher	[…]
Postadresse	[…]
Telefonnummer	[…]
E-Mail-Adresse	[…]

2 Beschreibung der beabsichtigten Bearbeitung von Personendaten

Welche (besonderen) Personendaten sollen bearbeitet werden (Datenkategorien)?
[…]

Wie sollen Personendaten bearbeitet werden (Bearbeitungsvorgänge)?
[…]

Zu welchem Zweck sollen Personendaten bearbeitet werden?
[…]

In welchem Umfang sollen Personendaten bearbeitet werden?
[…]

3 Risikoanalyse

Welche Risiken sind mit der geplanten neuen Bearbeitung von Personendaten verbunden?

1. […]
2. […]
3. […]

Liegen Faktoren vor, welche ein hohes Risiko für die Persönlichkeit oder Grundrechte betroffener Personen mit sich bringen können? Wenn ja, welche?

☐	automatisierte Einzelentscheidungen
☐	Bearbeitung von besonders schützenswerten Personendaten
☐	Verwendung neuer Technologien
☐	umfangreiche Bearbeitung besonders schützenswerter Personendaten

☐	Zusammenführen/Kombinieren von Personendaten, die durch unterschiedliche Prozesse gewonnen wurden
☐	Scoring/Profiling
☐	andere Risikofaktoren, welche zu einer hohen Gefährdung von Grundrechten betroffener Personen führen können: […]
☐	keine besonderen Risikofaktoren vorhanden

4 Bewertung von Risiken

Wie sind die identifizierten Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person in Bezug auf ihre *Schwere* zu bewerten?

	Bewertung		
Risiko	**gering**	**mittel**	**schwer**
1. […]	☐	☐	☐
2. […]	☐	☐	☐
3. […]	☐	☐	☐

Wie sind die identifizierten Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person in Bezug auf die *Wahrscheinlichkeit ihres Eintretens* zu bewerten?

	Bewertung		
Risiko	**gering**	**mittel**	**schwer**
1. […]	☐	☐	☐
2. […]	☐	☐	☐
3. […]	☐	☐	☐

5 Massnahmen zur Bewältigung der Risiken

Welche Massnahmen zur Bewältigung der identifizierten Risiken wurden bereits getroffen oder sind geplant?

	bereits getroffen:	geplant per:
[…]	☐ Dokumentation vorhanden	[…]
[…]	☐ Dokumentation vorhanden	[…]
[…]	☐ Dokumentation vorhanden	**[…]**
[…]	☐ Dokumentation vorhanden	[…]

[…]	☐ Dokumentation vorhanden	[…]
[…]	☐ Dokumentation vorhanden	[…]

6 Weiteres Vorgehen

Ergibt sich aus der Datenschutz-Folgenabschätzung, dass die geplante Bearbeitung trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hat, so ist eine Stellungnahme des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) einzuholen.

☐ **Projekt wird dem EDÖB zur Konsultation vorgelegt**

☐ **Konsultation des EDÖB nicht erforderlich**

Einleitende Bemerkung:

Vorliegend wird davon ausgegangen, dass die Auftragsdatenbearbeitungsvereinbarung direkt in einen Rahmenvertrag integriert wird. Diese kann auch als separate Anlage zum Hauptvertrag verfasst werden. In diesem Fall müsste im Rahmenvertrag auf die Anlage verwiesen werden, mit dem Hinweis, dass diese integrierender Bestandteil desselben darstellt. Sie finden die entsprechenden Textbausteine für beide Varianten untenstehend.

Die Vorlage ist sehr grundsätzlich und einfach formuliert. Sie sollte daher bei Bedarf – ggf. unter Einbezug eines Spezialisten – ergänzt werden. In jedem Fall sind die Angaben in [eckigen Klammern] situationsbezogen zu ersetzen bzw. zu entfernen.

* * * * *

[Titel/Einführung für Variante: Anlage zum Hauptvertrag]

Vereinbarung zur Auftragsdatenbearbeitung gemäss Art. 9 DSG: Anlage zum Hauptvertrag [X] vom [Datum]

Diese Vereinbarung zur Auftragsdatenbearbeitung wird abgeschlossen zwischen

[Firma, Anschrift des Verantwortlichen]

(im Folgenden „Verantwortlicher“)

und

[Firma, Anschrift des Auftragsbearbeiters]

(im Folgenden „Auftragsbearbeiter“)

[Übernehmen in Variante: Klausel im Rahmenvertrag]

Der Auftragsbearbeiter verpflichtet sich, die im Folgenden beschriebenen Datenbearbeitungen im Sinne von Art. 5 lit. d i.V.m. Art. 9 DSG im Auftrag des Verantwortlichen zu erbringen. Für die Zwecke dieser Vereinbarung gelten die Begriffsbestimmungen des Schweizer Datenschutzgesetzes (DSG).

1. Anwendungsbereich

[Variante: Klausel im Rahmenvertrag]

Im Rahmen des vorliegenden Vertrages können Daten des Verantwortlichen zum Zwecke der Bearbeitung dieser Daten in seinem Namen an den Auftragsbearbeiter übermittelt werden („Auftragsdaten“). Der Auftragsbearbeiter stellt einen angemessenen Schutz der an ihn übertragenen Personendaten sicher. Die Parteien halten bei der Bearbeitung von Daten im Zusammenhang mit diesem Vertrag die geltenden Vorschriften über die Bearbeitung von Personendaten, namentlich des Schweizer Datenschutzgesetzes (DSG), ein.

Diese Klausel gilt für alle Personendaten, die

- vom Verantwortlichen an den Auftragsbearbeiter übertragen (miteingeschlossen ist hierbei der Zugriff auf solche Daten) wurden oder
- vom Auftragsbearbeiter im Auftrag des Verantwortlichen bearbeitet werden.
- Bei den zu übertragenden und zu bearbeitenden Personendaten handelt es sich um:
  o […]
- [Variante: Die zu übertragenden und zu bearbeitenden Personendaten sind in Anhang [x] zu dieser Vereinbarung enthalten.]

[Variante: Anlage zum Hauptvertrag]

Bei der Erbringung der Leistungen gemäss dem Rahmenvertrag vom [Datum] verarbeitet der Auftragsbearbeiter Personendaten, die der Verantwortliche zur Erbringung der Leistungen zur Verfügung gestellt hat („Auftragsdaten"). Diese Anlage spezifiziert die Datenschutzpflichten und -rechte der Parteien im Zusammenhang mit der Bearbeitung der Auftragsdaten zur Erbringung der Leistungen nach dem Hauptvertrag.

[Ab hier für beide Varianten]

2. Umfang der Bearbeitung, Weisungsbefugnisse des Verantwortlichen

2.1 Der Auftragsbearbeiter bearbeitet die Auftragsdaten ausschliesslich so, wie der Verantwortliche selbst es tun darf.

2.2 Die Bearbeitung von Auftragsdaten durch den Auftragsbearbeiter erfolgt ausschliesslich in der Art, dem Umfang und zu dem Zweck [Zweck des Vertrages] / [bzw. wie in Anhang [x] zu diesem Vertrag [bzw. zu dieser Anlage] spezifiziert]; die Bearbeitung betrifft ausschliesslich die darin bezeichneten Arten von Personendaten und Kategorien betroffener Personen.

2.3 Die Dauer der Bearbeitung beträgt [Zeitraum]
[bzw. Die Dauer der Bearbeitung entspricht der Laufzeit des Rahmenvertrages.]

2.4 Der Verantwortliche behält sich das Recht zur Erteilung von Weisungen über Art, Umfang, Zwecke und Mittel der Bearbeitung von Auftragsdaten vor.

3. Anforderungen an Personal

3.1 Der Auftragsbearbeiter hat alle Personen, die Auftragsdaten verarbeiten, bezüglich der Bearbeitung von Auftragsdaten zur Vertraulichkeit zu verpflichten.

3.2 Der Auftragsbearbeiter stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Auftragsdaten haben, diese nur auf seine Anweisung verarbeiten, es sei denn, sie sind von Gesetzes wegen zur Bearbeitung verpflichtet.

4. Sicherheit der Bearbeitung

4.1 Der Auftragsbearbeiter ergreift alle geeigneten technischen und organisatorischen Massnahmen, die unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Bearbeitung der Auftragsdaten sowie der

unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Persönlichkeit und Grundrechte der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftragsdaten zu gewährleisten.

4.2 Der Auftragsbearbeiter hat vor dem Beginn der Bearbeitung der Auftragsdaten insbesondere die nötigen [bzw. in Anhang [y] zu dieser Anlage spezifizierten] technischen und organisatorischen Massnahmen zu ergreifen und während der Dauer des Hauptvertrags aufrechtzuerhalten sowie sicherzustellen, dass die Bearbeitung von Auftragsdaten im Einklang mit diesen Massnahmen durchgeführt wird.

5. Inanspruchnahme weiterer Auftragsbearbeiter

5.1 Der Verantwortliche genehmigt hiermit in allgemeiner Weise die Inanspruchnahme weiterer Auftragsbearbeiter durch den Auftragsbearbeiter. Die gegenwärtig vom Auftragsbearbeiter eingesetzten weiteren Auftragsbearbeiter sind nachfolgend [bzw. in Anhang [z]] genannt: [Auflistung] [bzw. Der Verantwortliche erlaubt dem Auftragsbearbeiter nicht, weitere Auftragsbearbeiter zur Bearbeitung der Auftragsdaten beizuziehen. *Diesfalls 5.2 löschen.*]

5.2 Der Auftragsbearbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsbearbeiter. Der Verantwortliche kann Widerspruch gegen diese Änderung erheben. Erhebt der Verantwortliche Widerspruch, ist dem Auftragsbearbeiter die beabsichtigte Änderung untersagt. Im Falle zugelassener Änderungen wird der Auftragsbearbeiter die Liste der Unter-Auftragsbearbeiter gemäss Ziff. 5.1 entsprechend aktualisieren und dem Verantwortlichen unverlangt zur Verfügung stellen.

5.3 Der Auftragsbearbeiter wird jedem weiteren Auftragsbearbeiter vertraglich dieselben Datenschutzpflichten auferlegen, die in diesem Vertrag [bzw. dieser Anlage] in Bezug auf den Auftragsbearbeiter festgelegt sind.

5.4 Der Auftragsbearbeiter wird vor jeder Beauftragung sowie regelmässig während der Beauftragung überprüfen, dass die weiteren Auftragsbearbeiter geeignete technische und organisatorische Massnahmen ergriffen haben und diese so durchgeführt werden, dass die Bearbeitung der Auftragsdaten gemäss diesem Vertrag [bzw. dieser Anlage] erfolgt.

6. Rechte der betroffenen Personen

6.1 Der Auftragsbearbeiter wird den Verantwortlichen im Rahmen des Zumutbaren dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.

6.2 Der Auftragsbearbeiter wird insbesondere:

- den Verantwortlichen unverzüglich informieren, falls sich eine betroffene Person mit einem Antrag auf Wahrnehmung ihrer Rechte in Bezug auf Auftragsdaten unmittelbar an den Auftragsbearbeiter wenden sollte;

- dem Verantwortlichen auf Anfrage alle bei ihm vorhandenen Informationen über die Bearbeitung von Auftragsdaten geben, die der Verantwortliche zur Beantwortung des Antrags einer betroffenen Person benötigt und über die der Verantwortliche nicht selbst verfügt.

7. Sonstige Unterstützungspflichten des Auftragsbearbeiters

7.1 Der Auftragsbearbeiter meldet dem Verantwortlichen so rasch als möglich jede Verletzung der Datensicherheit, insbesondere Vorkommnisse, die zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu Auftragsdaten führen.

7.2 Für den Fall, dass der Verantwortliche verpflichtet ist, die Aufsichtsbehörde EDÖB nach Art. 24 DSG (Meldung von Verletzungen der Datensicherheit) zu informieren, wird der Auftragsbearbeiter den Verantwortlichen auf dessen Anfrage hin unterstützen, diese Pflichten einzuhalten.

8. Datenlöschung und -rückgabe

Der Auftragsbearbeiter wird auf die Weisung des Verantwortlichen hin mit Beendigung des Hauptvertrages alle Auftragsdaten entweder vollständig und unwiderruflich löschen oder an den Verantwortlichen zurückgeben, sofern nicht gesetzlich eine Verpflichtung des Auftragsbearbeiters zur weiteren Speicherung der Auftragsdaten besteht.

9. Nachweise und Überprüfungen

9.1 Der Auftragsbearbeiter hat sicherzustellen, dass die Bearbeitung der Auftragsdaten mit diesem Vertrag [bzw. dieser Anlage], [einschliesslich des in Anhang [x] festgelegten Umfangs der Bearbeitung der Auftragsdaten,] sowie den Weisungen des Verantwortlichen in Einklang steht.

9.2 Der Auftragsbearbeiter führt ein Bearbeitungsverzeichnis der Auftragsdaten. Dieses wird auf Anfrage hin dem Auftraggeber zugänglich gemacht.

[ggf. Ort, Datum, Unterschriften]

Einleitende Bemerkung:

Die vorliegende Musterklausel ist an die jeweiligen individuellen Bedürfnisse und Gegebenheiten anzupassen. Insbesondere konkrete Bearbeitungszwecke sind zu ergänzen, sofern diese noch nicht aufgelistet sind. Diese sollten auch mit der Datenschutzerklärung abgeglichen werden. Falls nötig kann dazu ein Spezialist beigezogen werden.

Namentlich die Angaben in [eckigen Klammern] müssen an Ihre konkrete Situation angepasst werden.

* * * * *

Musterklausel Datenschutz in AGB

[Ziff.] Datenschutz

Im Zusammenhang mit der Erbringung von Dienstleistungen [und/oder Verkauf von Produkten] für den Kunden kann [Firma] unter jederzeitiger Beachtung geltender Datenschutznormen Personendaten selbst erheben, von Dritten beschaffen, speichern, bearbeiten und an Dritte weitergeben.

Wenn gesetzlich erlaubt, oder überwiegende Interessen seitens [Firma] bestehen, oder eine Kundeneinwilligung vorliegt, kann [Firma] die erhobenen Personendaten für folgende Zwecke bearbeiten:

a) zur Überprüfung von Voraussetzungen für einen Vertragsabschluss;

b) zur Erfüllung von vertraglichen Verpflichtungen gegenüber dem Kunden;

c) zur Pflege, Entwicklung und Erhaltung der Kundenbeziehung;

d) um Dienste zu individualisieren oder personalisierte Inhalte bereitzustellen z.B. mittels Untersuchung hinsichtlich der Demographie, des Nutzungsverhaltens und der Nutzerinteressen;

e) zur Adressvalidierung.

f) zur Verhinderung einer unrechtmässigen Benutzung von Dienstleistungen (insbesondere zur Verhinderung von Betrugsfällen beim Vertragsschluss und während der Dauer des Vertrags);

g) zur Rechnungsstellung, zu Inkassozwecken und für Bonitäts- und Kreditwürdigkeitsprüfungen;

h) zur Bewerbung, Gestaltung und Weiterentwicklung von [Firma]-Produkten;

j) [ggf. weitere Zwecke].

[Firma] darf Dritte im In- und Ausland zur Datenbearbeitung beziehen. [Bezieht der Kunde bei [Firma] Dienstleistungen Dritter, darf [Firma] dem Dritten diejenigen Kundendaten zur Bearbeitung weitergeben, die dieser zur Erfüllung der vertraglichen Verpflichtungen gegenüber dem Kunden benötigt.][1]

[1] In der Mustervorlage der Datenschutzerklärung wird festgehalten, dass keine Daten weitergegeben werden. Dies bezieht sich grundsätzlich ausschliesslich auf Daten, welche im Zusammenhang mit der Website beschafft werden und muss nicht im Widerspruch zu der vorliegenden Bestimmung stehen. Ggf. sind die Bestimmungen aber anzugleichen.

Beim Beizug von Dritten aus dem In- und Ausland durch [Firma] sind diese entsprechend vertraglich verpflichtet, die gemäss gültigem Datenschutzrecht notwendigen Massnahmen einzuhalten. Weitere Information betreffend Verwendung von Personendaten sind in der Datenschutzerklärung unter [Link] enthalten.