Balmer Etienne

Ratgeber Datenschutz

für Unternehmen

TREUHAND · PRÜFUNG · BERATUNG

Zum **1. September 2023** tritt das neue Datenschutzgesetz (DSG) der Schweiz ohne Übergangsfrist in Kraft. Die **Datenschutz-Compliance-Anforderungen** für Unternehmen werden erhöht, die **Governance-Struktur** ist anzupassen.

Dieser **Ratgeber** zeigt **privaten Unternehmen** (nachfolgend "Unternehmen") auf, welche erhöhten Anforderungen **risikobasiert** neu umzusetzen sind. Nicht eingegangen wird auf die Datenschutz-Grundverordnung der EU (DSGVO) sowie auf die kantonalen Datenschutzgesetze. Weitere Infos und Tipps sind unter www.balmer-etienne.ch abrufbar. Bei Fragen hilft Ihnen unser Datenschutz-Team gerne weiter (datenschutz-beratung@balmer-etienne.ch oder +41 41 228 11 11).

Inhaltsverzeichnis

1. Ziele des DSG

Was		Wie / Warum
Schutz der Persönlichkeit und Grundrechte von natürlichen Personen (Schutz von juristischen Personen entfällt)	→	Verbesserung der Transparenz der Datenbearbeitung und Stärkung der persönlichen Selbstbestimmung über Personendaten
Angleichung an die europäische Gesetzgebung	→	Formlose grenzüberschreitende Datenbekanntgabe soll weiterhin möglich sein

Datenschutz wurde an die veränderten **technologischen** und **gesellschaftlichen Verhältnisse** angepasst.

2. Folgen für Unternehmen

- **Erhöhung der Compliance-Anforderungen,** namentlich durch Ausdehnung der Informations- und Auskunftspflichten, der Dokumentationsanforderungen, der Datensicherheitsvorschriften sowie der Meldepflicht von Datensicherheitsverletzungen.
- **Verschärfung der Strafbestimmungen,** namentlich höhere Bussen, persönliche Haftung, Verwaltungsverfahren infolge Stärkung der Kompetenzen der Aufsichtsbehörde mit Kostenfolgen.

3. Wichtige datenschutzrechtliche Begriffe

Personendaten: Alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Darunter fallen persönliche Angaben wie Vorname, Name, Geburtsdatum, Adresse, Heimatort, Zivilstand, Telefonnummer, E-Mailadresse, Fotos, aber auch URL-Adressen etc.

Verantwortlicher: Person oder Organisation, die über die Bearbeitung der Personendaten entscheidet.

Betroffene Person: Natürliche Person, deren Personendaten bearbeitet werden. Darunter fallen insbesondere bestehende und ehemalige Mitarbeitende, Stellensuchende, Ansprechpersonen bei bestehenden und potentiellen Kunden und Lieferanten.

Auftragsbearbeiter: Dienstleister, der im Auftrag des Verantwortlichen Personendaten bearbeitet (z.B. IT-Dienstleister).

Bearbeitung: Jeder Umgang mit Personendaten, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Personendaten.

Besonders schützenswerte Personendaten: Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, genetische Daten, biometrische Daten etc.

DSGVO: Datenschutz-Grundverordnung der EU (das Pendant zum DSG in der Schweiz).

Technische und organisatorische Massnahmen (TOM): Technische Massnahmen, welche das Informationssystem wie Zutrittskontrollen, Netzsicherheit, Sperrbildschirm etc. betreffen sowie organisatorische Massnahmen, welche das Systemumfeld wie Mitarbeitersensibilisierung, interne Weisungen etc. umfassen, zur Gewährleistung der Datensicherheit.

Datenschutz-Folgenabschätzung (DSFA): Die DSFA ist ein Compliance-Instrument, welches in datenschutzrechtlicher Selbstbeurteilung die Datenbearbeitung, das Risiko für die Persönlichkeit der betroffenen Personen sowie die Massnahmen zu deren Schutz beschreibt und analysiert. Bei einem hohen Risiko für die betroffenen Personen ist eine DSFA Pflicht.

EDÖB: Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) ist die beratende und beaufsichtigende Anlaufstelle nach dem schweizerischen Datenschutzgesetz. Er ist auch die Meldestelle für Datensicherheitsvorfälle.

4. Die Pflichten des Verantwortlichen

Anwendbarkeit DSG

Das Bearbeiten von Personendaten durch Unternehmen unterliegt dem DSG, unabhängig von den angewandten Verfahren oder Mitteln (physisch auf Papier, digitalisiert in Softwaretools). In der Privatwirtschaft bedürfen Personendatenbearbeitungen grundsätzlich weder einer Einwilligung noch sonstiger Rechtfertigungsgründe.

Wann braucht es einen Rechtfertigungsgrund

Ein **Rechtfertigungsgrund** ist nur dann notwendig, wenn entweder

- die **Bearbeitungsgrundsätze nicht eingehalten** werden,
- die **betroffene Person** der Bearbeitung **widerspricht** oder
- **besonders schützenswerte Personendaten** mitgeteilt werden sollen.

Empfehlung: Datencheck

Hier weicht das Schweizer Datenschutzrecht von der DSGVO ab. Diese setzt in jedem Fall einen Rechtsfertigungsgrund voraus. Um Personendaten **datenschutzkonform** zu bearbeiten, hat sich der Verantwortliche **risikobasiert** pro Prozess (Bewerber, Mailings usw.) die folgenden Fragen zu stellen:

Datencheck		Beispiele
Wo werden	→	CRM, Outlook
welche Personendaten	→	Mailadressen, Namen, Vornamen
für welchen Zweck bearbeitet?	→	Newsletter-Versand

Ein Unternehmen hat dabei die folgenden Pflichten:

4.1 Einhaltung der Bearbeitungsgrundsätze bzw. Vorliegen eines Rechtfertigungsgrundes

4.2 Informationspflichten: Das Unternehmen informiert die betroffenen Personen vorgängig, was mit den Personendaten wozu gemacht wird

4.3 Einhaltung der Betroffenenrechte

4.4 Meldepflicht bei einem Datensicherheitsvorfall beim EDÖB

4.5 Datenschutz-Folgenabschätzung (DSFA) bei hohem Risiko für die betroffenen Personen

4.6 Führen eines Bearbeitungsverzeichnisses

4.1 Bearbeitungsgrundsätze bzw. Vorliegen eines Rechtfertigungsgrundes

Ein Unternehmen hat die folgenden Bearbeitungsgrundsätze einzuhalten:

Rechtmässigkeit
Jede Bearbeitung von Personendaten muss sämtliche Bestimmungen des Schweizer Rechts einhalten, welche direkt oder indirekt den Schutz der Persönlichkeit bezwecken (bspw. Recht am eigenen Bild).

Zweckbindung
Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei deren Beschaffung für die betroffene Person erkennbar, aus den Umständen ersichtlich bzw. mit diesem Zweck vereinbar ist. Ist der Zweck erreicht, sind die Daten zu löschen (**Löschkonzept**).

Treu und Glauben sowie **Transparenz**
Die betroffene Person muss wissen oder erkennen können, welche Personendaten zu welchem Zweck beschafft werden. **Kein heimliches Beschaffen.**

Verhältnismässigkeit
Die Datenbearbeitung muss für den verfolgten Zweck notwendig und im Hinblick auf eine potentielle Persönlichkeitsverletzung vernünftig sein. Es sind nur die notwendigen Persondaten für die Erreichung des Zwecks zu bearbeiten (**Datenminimierung**). **Keine Datensammlung auf Vorrat.**

Datenrichtigkeit und **Datensicherheit**
Der Verantwortliche ist für die Richtigkeit der Personendaten verantwortlich. Mittels geeigneten technischen und organisatorischen Massnahmen (TOM) hat der Verantwortliche sicherzustellen, dass unrichtige Personendaten berichtigt, gelöscht oder vernichtet sowie die Personendaten vor jeder unbefugten Bearbeitung geschützt werden.

Privacy by design und **Privacy by default**
Der Verantwortliche ist verpflichtet, die Bearbeitung von Personendaten von Anfang an datenschutzkonform zu bearbeiten und die nach Stand der Technik angemessenen Massnahmen zu treffen. Bei Software-Anwendungen mit einer Wahlmöglichkeit hat er bei der Standardeinstellung die am wenigsten weitgehende Einstellung (kleinste Datenmenge) zu wählen.

Hält ein Unternehmen einen Bearbeitungsgrundsatz nicht ein, ist dafür einer der folgenden **Rechtfertigungsgründe** notwendig:

Einwilligung: Die betroffene Person hat in die Bearbeitung freiwillig und informiert einzuwilligen. Bei der Einholung der Einwilligung sind formelle Anforderungen zu beachten. Einwilligungen sind jederzeit widerrufbar!

oder

Grundlage im Schweizer Recht, welche die Bearbeitung rechtfertigt (Unternehmen bearbeiten z.B. Personendaten für die Behörden [AHV, IV etc.]).

oder

Überwiegendes privates Interesse: Die Interessen der betroffenen Person und des Unternehmens werden gegen übergestellt und ihre Datenschutzinteressen abgewogen. Das Gesetz nennt exemplarische Beispiele von überwiegend privaten Interessen wie Bearbeitungen im Zusammenhang mit einem Vertragsabschluss und -abwicklung, bei der Prüfung der Kreditwürdigkeit, Bearbeitung von Konkurrentendaten, Rechtfertigungsgrund der Medien (Art. 31 Abs. 2 DSG).

4.2 Informationspflichten

Bei jeder Beschaffung von Personendaten muss ein Unternehmen die betroffenen Personen **angemessen informieren**. Dabei ist zwischen dem Mindestinhalt und erweiterter Informationspflicht im Einzelfall zu unterscheiden.

	Was		Informationspflicht
Mindest-inhalt	Wer ist verantwortlich?	→	Die Identität und die Kontaktdaten des Unternehmens
	Wozu werden die Personendaten beschafft?	→	Der Bearbeitungszweck
Einzelfälle +	Datenbekanntgabe an Dritte	→	Empfänger oder Kategorien der Empfänger (Namensnennung nicht nötig)
	Personendaten nicht bei betroffenen Personen beschafft	→	Kategorien der bearbeiteten Personendaten
	Bekanntgabe von Personendaten ins Ausland	→	Land/Länder/Region und Garantien zur Gewährleistung des Datenschutzniveaus
	DSFA (Aufsichtsbehörde [EDÖB] soll nicht konsultiert werden)	→	Kontaktdaten des Datenschutzberaters
	Ausländisches Unternehmen	→	Name und Adresse des Schweizer Vertreters
	Automatisierte Einzelfallentscheidung	→	Information der betroffenen Person

Damit soll eine transparente Datenbearbeitung gewährleistet werden. Der Mindestinhalt geht im Schweizer Datenschutzgesetz weniger weit als in der DSGVO. Jedoch sind die Pflichtangaben bei Bekanntgabe von Personendaten ins Ausland weitergehend.

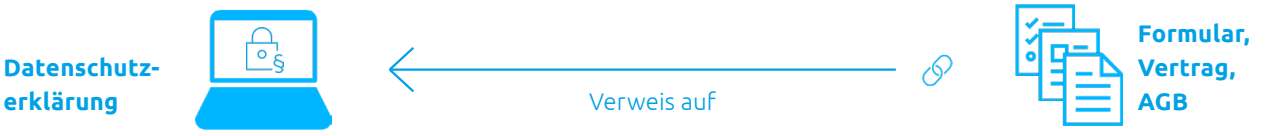
Ausnahmen

Die Informationspflicht entfällt in den folgenden Fällen:

- Personendaten werden vom Unternehmen **ungewollt oder zufällig erfasst**. Die Erfassung war nicht geplant, z.B. Erhalt von Visitenkarten oder E-Mails.
- Die Beschaffung der Personendaten fällt unter einen **gesetzlichen Ausnahmetatbestand** wie namentlich **betroffene Person ist bereits informiert, gesetzlich vorgesehene Bearbeitung** oder **unverhältnismässiger Aufwand.**

Umsetzung

Die Informationspflicht unterliegt **keiner Formvorschrift** und erfolgt am einfachsten mit einer **Datenschutzerklärung auf der Webseite**.



Wichtig ist, dass die Datenschutzerklärung auf der Webseite schnell und einfach gefunden wird sowie vollständig und verständlich ist.

4.3 Betroffenenrechte

Ein Unternehmen hat die folgenden Betroffenenrechte sicherzustellen:

Bestehende Rechte

Recht auf Berichtigung
Personendaten sind auf Antrag der betroffenen Person zu korrigieren.

Recht auf Löschung/Vergessen werden
Personendaten sind auf Antrag der betroffenen Person zu löschen, die Bearbeitung oder Weitergabe wird verboten.

Berichtigungsvermerk
Auf Antrag der betroffenen Person ist im System ein Vermerk aufzunehmen, dass die betroffene Person die Richtigkeit bestreitet.

Anzeigerecht
Jeder kann Anzeige erstatten.

Neue oder erweiterte Rechte

Auskunftsrecht

Was

Firma und Kontaktdaten des Unternehmens	Bearbeitete Personendaten	Aufbewahrungsdauer oder Kriterien dazu	Bearbeitungs-zweck	Herkunft der Personendaten
Vorliegen einer automatisierten Einzelfallentscheidung inkl. Entscheidungslogik	Empfänger bzw. Kategorien der Empfänger bei Bekanntgabe	Grund der Auskunftsverweigerung, -einschränkung, -aufschiebung		

Wie

- **kostenlos** (Ausnahme: Bei unverhältnismässigem Aufwand ist Kostenbeteiligung bis CHF 300 zulässig)
- **innert 30 Tagen** (Ausnahmen möglich)
- **grundsätzlich schriftlich (auch elektronisch)**

Ausnahmen

Das Unternehmen **kann die Auskunft** nur in engen **Ausnahmefällen verweigern, einschränken oder aufschieben**, z.B. wenn es um den Schutz eines Berufsgeheimnisses geht, überwiegende Interessen Dritter dies erfordern oder das Auskunftsbegehren offensichtlich unbegründet und damit entweder querulatorisch oder datenschutzwidrig ist. Letzteres ist gegeben, wenn es um Abklärung von Prozessaussichten oder Sammlung von Beweisen für einen möglichen Prozess geht. Der Ausnahmegrund ist anzugeben.

Datenportabilität

Was

Herausgabe der Personendaten in einem gängigen elektronischen Format an die betroffene Person oder Übertragung an einen Dritten.

Warum

Damit soll es Nutzern von Online-Diensten erleichtert werden, Personendaten, die sie dem Verantwortlichen bekannt gegeben haben (z.B. eine Playlist), einfach von einem Dienstleister auf einen anderen zu verschieben. Voraussetzung dafür ist, dass die Personendaten automatisiert bearbeitet und auf der Grundlage einer Einwilligung oder der Erfüllung eines Vertrages bearbeitet wurden.

Recht auf menschliches Gehör

Was

Anspruch auf Beurteilung durch eine natürliche Person bei automatisierten Einzelfallentscheidungen.

Wie

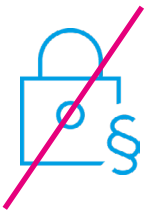
In den engen Grenzen einer automatisierten Einzelfallentscheidung, insbesondere in den Fällen, wo Entscheidungen ausschliesslich aufgrund Künstlicher Intelligenz (KI) automatisiert getroffen werden, hat die betroffene Person das Recht, dass diese Entscheidung durch eine natürliche Person überprüft wird. Dies kann in der Praxis beispielsweise relevant sein, wenn Bewerbungen von Stellensuchenden automatisiert abgelehnt oder Blutwerte im medizinischen Bereich automatisiert ausgewertet werden.

Umsetzung

Das Unternehmen identifiziert die betroffene Person. Wie bisher wird das **Auskunftsrecht** neben dem Anzeigerecht an die Aufsichtsbehörde EDÖB das **bedeutendste** Recht bleiben. Denn nur wer weiss, ob und welche Personendaten über ihn bearbeitet werden, kann diese nötigenfalls berichtigen bzw. vernichten lassen oder wenigstens deren Richtigkeit bestreiten. Hier sind **Prozesse** notwendig, die den administrativen Aufwand verringern, Personalressourcen schonen und sicherstellen, dass die Betroffenenrechte eingehalten werden.

4.4 Meldepflichten beim Datensicherheitsvorfall

Datensicherheitsvorfall – was ist zu tun?



Meldung an die Aufsichtsbehörde EDÖB

Ein Unternehmen muss **neu** eine Verletzung der Datensicherheit, die voraussichtlich zu einem **hohen Risiko** für die Persönlichkeitsrechte der betroffenen Personen führt, dem **EDÖB** melden. Ob ein hohes Risiko vorliegt, ist im Einzelfall zu beurteilen. Die Meldung muss dabei so **rasch als möglich** (aber nicht zwingend innert 72 Stunden) erfolgen.

Information der betroffenen Personen

Wenn es zum Schutz der betroffenen Personen notwendig ist oder der EDÖB es verlangt, muss das Unternehmen zudem die betroffenen Personen selber informieren. **Ausnahme bei übermässigem Aufwand!**

Eine solche Information soll ausnahmsweise erforderlich sein, wenn z.B. die betroffene Person selber tätig werden muss, um die Folgen der Datensicherheitsverletzung zu verringern (ändern des Passworts).

Voraussetzung und Umsetzung

Eine **Datensicherheitsverletzung** liegt im Wesentlichen vor, wenn im Rahmen einer Datenbearbeitung in unvorhergesehener Weise die Vertraulichkeit, Integrität oder Verfügbarkeit von Personendaten beeinträchtigt wird und dies dazu führt, dass Personendaten unbeaufsichtigt sind, verlorengehen, gelöscht, vernichtet, verändert, Unbefugten offengelegt oder zugänglich gemacht werden. **Wichtig dabei zu wissen**: Die **Möglichkeit einer Datensicherheitsverletzung** reicht bereits aus. Ein Nachweis, dass eine Verletzung stattgefunden hat, ist nicht Voraussetzung für das Bejahen einer Meldepflicht.

Im Zeitalter von nahezu täglichen **Cyber-Crime Angriffen** kann es schnell passieren, dass Personendaten unerlaubterweise abgezogen oder gestohlen werden. Die Gefahr einer Verletzung **geht aber hauptsächlich von Mitarbeitenden aus**, die ihre Kompetenzen missbrauchen oder unvorsichtig handeln.

Aktuelle technische und organisatorische Massnahmen (TOM) sind ein guter Schutz gegen Datensicherheitsverletzungen.

technische Beispiele	organisatorische Beispiele
Zugang „need to know“	Weisungen
persönliches Konto	Reglemente
Authentifizierung	Schulungen
Firewall	

4.5 Datenschutz-Folgenabschätzung (DSFA)

Voraussetzung

Unternehmen müssen **vor** der Datenbearbeitung eine **Datenschutz-Folgenabschätzung** (DSFA) durchführen, wenn die Art, der Umfang, die Umstände und der Zweck der beabsichtigten Datenbearbeitung ein **hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person** mit sich bringt («heikle Datenbearbeitungen»). Das kann durch Einsatz neuer digitaler Technologien (Künstliche Intelligenz [KI]), in Fällen der umfangreichen Bearbeitung besonders schützenswerter Personendaten oder bei der systematischen Überwachung (z.B. Videoüberwachung von Mitarbeitenden) der Fall sein.

Ausnahmen

Ein Unternehmen darf von einer DSFA Abstand nehmen, wenn

- es **gesetzlich** zur Bearbeitung der Personendaten **verpflichtet** ist;
- ein **Produkt, System oder eine Dienstleistung** nach den neuen Regelungen **zertifiziert** ist, oder wenn
- es einen geprüften **Verhaltenskodex** einhält.

Kommt ein Unternehmen nach Durchführung einer DSFA zum Schluss, dass die geplante Bearbeitung trotz der vorgesehenen Massnahmen immer noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen darstellt, ist entweder der ernannte Datenschutzberater oder der EDÖB zu konsultieren. Diese nehmen zur geplanten Bearbeitung Stellung. Bestehen datenschutzrechtliche Einwände gegen die geplanten Bearbeitungen als solche, schlägt der EDÖB (bzw. der Datenschutzberater) dem Unternehmen geeignete Massnahmen zur Modifizierung vor, so dass das Risiko nicht mehr hoch ist.

4.6 Bearbeitungsverzeichnis

Vorteile eines Bearbeitungsverzeichnisses

Das Wissen, welche Personendaten ein Unternehmen wie und wofür bearbeitet, ist die Basis für einen verantwortungsvollen Datenschutz.

Mit einem **aktuellen Bearbeitungsverzeichnis** kann ein Unternehmen seine Pflichten als Verantwortlicher, insbesondere die strafbewährten Pflichten wie Datensicherheit, Datenbekanntgabe sowie Informations- und Auskunftspflichten, besser einhalten.

Pflicht und Ausnahme

Unternehmen sind grundsätzlich verpflichtet, ein **Bearbeitungsverzeichnis** zu führen. Dafür entfällt die Registrierungspflicht der Datensammlung beim EDÖB. Unternehmen mit weniger als 250 Beschäftigten und wenn keine besonders schützenswerte Personendaten in grossem Umfang vorliegen oder Profiling mit hohem Risiko durchgeführt werden, sind von dieser Pflicht befreit. Das Verzeichnis muss **schriftlich** geführt werden, wobei eine **elektronische Form genügt** (Excel Sheet, Software).

Mindestinhalt

Der Mindestinhalt eines Bearbeitungsverzeichnisses ist davon abhängig, ob das Unternehmen Verantworlicher oder Auftragsbearbeiter ist.

Unternehmen als Verantwortlicher	Unternehmen als Auftragsbearbeiter
Identität des Verantwortlichen	Identität des Verantwortlichen
Bearbeitungszweck	Identität des Auftragbearbeiters
Kategorien (betroffene Personen, bearbeitete Personendaten)	Kategorien der Bearbeitungen, die im Auftrag des Verantwortlichen durchgeführt werden
Aufbewahrungsdauer oder Kriterien zur Festlegung der Dauer	-
Kategorien der Empfänger	-
Beschreibung der Datensicherheitsmassnahmen (Verweis auf IT-Sicherheitsrichtlinie, TOM)	Beschreibung der Datensicherheitsmassnahmen (Verweis auf IT-Sicherheitsrichtlinie, TOM)
Bei Auslandsbekanntgabe: Angabe des Staates und Garantien zur Gewährleistung eines angemessenen Datenschutzes	Bei Auslandsbekanntgabe: Angabe des Staates und Garantien zur Gewährleistung eines angemessenen Datenschutzes

5. Auftragsdatenbearbeitungsvertrag

Wenn ein Unternehmen seine **eigene Datenbearbeitung** durch einen **Dritten** in **seinem Auftrag** ausführen lässt (z.B. IT-Dienstleister, Werbeversand), handelt es sich um eine Auftragsdatenbearbeitung. Dieses Outsourcing ist zulässig, solange der Auftragsbearbeiter die Bearbeitung ausschliesslich so bearbeitet, wie es das Unternehmen tun darf und keine gesetzlichen oder vertraglichen Geheimhaltungspflichten die Bearbeitung verbieten.

Ein **Auftragsdatenbearbeitungsvertrag (ADV)** sollte mindestens Folgendes beinhalten:

6. Geheimhaltungsverpflichtung

Eine Zusammenarbeit mit **Dritten** kann auch in der Form stattfinden, dass diese nicht als Auftragsbearbeiter arbeiten, aber dennoch Zugriff auf **Personendaten** und **Fabrikations-Geschäftsgeheimnisse** haben (z.B. Lieferanten, Berater). Mit einer **Geheimhaltungsverpflichtung (vielfach bekannt auch als NDA – Non-Disclosure-Agreement)** kann sichergestellt werden, dass die betroffenen Daten (Personendaten und weitere Daten) geschützt bleiben.

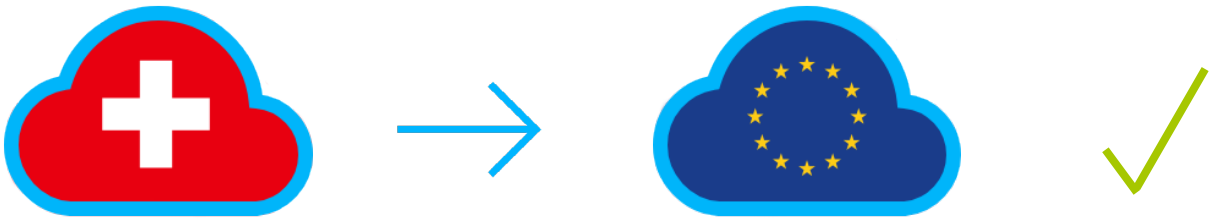
Eine **Geheimhaltungsverpflichtung** sollte mindestens Folgendes beinhalten:

- Kurze Umschreibung der geheimzuhaltenden Daten/Informationen
- Der Dritte verpflichtet sich, die Daten/Informationen nicht für sich zu bearbeiten
- Das Datengeheimnis besteht auch nach Beendigung der Zusammenarbeit
- Eine Weitergabe von Daten ist nur im gesetzlich erlaubten Umfang oder gemäss den vertraglich vereinbarten Regelungen erlaubt
- Löschpflicht/Rückgabepflicht regeln
- Anwendbares Recht und Gerichtsstand festlegen

7. Datenbekanntgabe ins Ausland

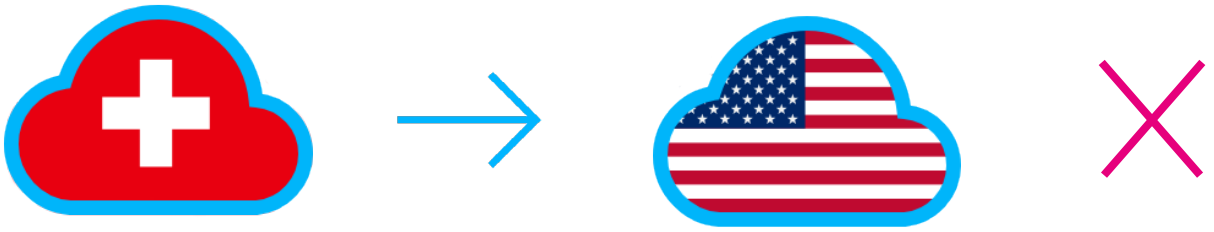
Grundsatz

Unternehmen dürfen Personendaten wie Mitarbeiterdaten ins Ausland bekannt geben (speichern auf Servern im Ausland, z.B. in der Cloud), solange diese Daten im Empfängerland angemessen, also mindestens in einem vergleichbaren Umfang wie in der Schweiz, geschützt sind (z.B. EU). Der Bundesrat legt in der Verordnung zum Datenschutzgesetz verbindlich fest, welche Länder einen angemessenen Datenschutz haben und der Datenexport daher ohne besondere Vorkehrungen erlaubt ist.



Garantien und Ausnahmen

Gilt ein Land nicht als sicher (z.B. USA), so muss durch hinreichende **Garantien** ein geeigneter Datenschutz gewährleistet werden. In den meisten Fällen wird mit den sogenannten **Standardvertragsklauseln (SCC)** gearbeitet, die auch in der Schweiz durch den EDÖB anerkannt sind oder es liegt ein **gesetzlicher Ausnahmetatbestand** wie eine **ausdrückliche Einwilligung, ein unmittelbarer Zusammenhang mit dem Abschluss oder Abwicklung eines Vertrages**, die Wahrung überwiegender öffentlicher Interesse oder die Durchsetzung von Rechtsansprüchen vor.



Umsetzung

In der Praxis sind Unternehmen insbesondere bei der IT-Struktur an grosse Softwareanbieter wie Microsoft Office 365 gebunden. Dies führt in den meisten Fällen zu einem Datenabfluss in das (nicht-europäische) Ausland und damit oft in Länder ohne angemessenes Datenschutzniveau (USA). Die dortige (Weiter-)Bearbeitung kann das Unternehmen weder kontrollieren noch ausschliessen. Risikobasiert sind die ausländischen Softwareanbieter einzubinden, wobei vorzugsweise Anbieter mit Sitz in der EU oder der Schweiz zu wählen sind, so dass die Daten in der EU oder in der Schweiz gespeichert werden. Zudem sind die betroffenen Personen transparent darüber zu informieren und ihre Einwilligung ist einzuholen.

8. Internetauftritt eines Unternehmens

Jedes Unternehmen nutzt das Internet für seine Firmenwebseite. Aus **datenschutzrechtlichen Überlegungen** sind dabei die folgenden Punkte zu beachten:

Inhalte der Webseite	Was gilt es zu beachten
Reine Informationsseite	Keine spezifische Vorkehrungen nötig.
Waren, Werke oder Leistungen werden angeboten.	• Geltungsbereich der DSGVO ist zu prüfen • Impressumspflicht • Spezielle Regelungen bei einem Webshop
Mitarbeiterfotos und deren Kontaktdaten	Veröffentlichung von Mitarbeiterfotos oder andere personenbezogene Daten bedürfen grundsätzlich einer **Einwilligung.** **Wichtig**: Gilt auch auf sozialen Netzwerken wie Unternehmensseiten auf LinkedIn, Twitter, Instagram, Facebook etc.
Kontaktformular / Online-Anmeldungen	Formulare unterliegen den datenschutzrechtlichen Bearbeitungsgrundsätzen, insbesondere der **Zweckbindung** sowie der **Datensparsamkeit**. **Hinweis auf der Datenschutzerklärung** ist notwendig.
Newsletter	Kein Newsletterversand ohne **Einwilligung** und **Widerrufsrecht**!
Impressum	**Keine generelle Impressumspflicht in der Schweiz**. Dies im Unterschied zur EU. Dort geht die Impressumspflicht weiter als in der Schweiz. Von den Betreibern von Webseiten werden klare und vollständige Angaben über deren Identität sowie eine Post- und E-Mailadresse gefordert, sofern sie **Waren, Werke oder Leistungen im elektronischen Geschäftsverkehr** anbieten. Dies ist bei Unternehmens-Webseiten meistens der Fall.
Datenschutzerklärung	Mit der Datenschutzerklärung erfüllt das Unternehmen seine **Informationspflicht** gemäss Datenschutzgesetz! **Wichtig**: Die Datenschutzerklärung ist so zu platzieren, dass sie durch den Besucher **schnell und mit wenigen Klicks** gefunden wird. Sie muss **einfach und verständlich sein**.
Analytic Tools und Cookies	Der Benutzer wird überwacht, wie er die Webseite nutzt. Mit der **Datenschutzerklärung** und gegebenenfalls dem **Cookie-Banner /** einer **Cookie-Policy** ist der Benutzer darüber zu informieren. **Wichtig**: Unterschiedliche Regelung in der Schweiz und in der EU. Die EU-Regelung ist strenger.

9. Mitarbeiterinformation

Das Unternehmen als Arbeitgeber bearbeitet im HR eine Vielzahl Personendaten. Es betrifft dies die Personendaten aus Bewerbungen wie auch aktiver oder ehemaliger Beschäftigter. Die Datenmenge ist dabei genauso beträchtlich wie der Bearbeitungszeitraum. Zudem werden im HR stets auch besonders schützenswerte Personendaten, z.B. über die Gesundheit, bearbeitet. Diese Daten gilt es wie bisher zu schützen.

Das Unternehmen als Arbeitgeber ist datenschutzrechtlich verpflichtet, die betroffene Person angemessen über die Beschaffung der Daten zu informieren.

Der Bearbeitungszweck und die sich daraus ergebende Informationspflicht ist abhängig vom Status der betroffenen Person. Dabei gilt im Arbeitsbereich generell die **Datenminimierungspflicht** (nur so viele Daten wie nötig, wobei so wenige wie möglich)!

Betroffene Personen	Bearbeitungszweck (Auszug)	Informationspflicht (Was und wie)
Job-Interessierte	Aufnahme in Karriere-Pool / Job-Newsletter	• Name des Verantwortlichen • Bearbeitungszweck • Empfänger der Daten und deren Ort (z.B. Newsletter-Dienstleister mit Sitz in den USA) **Einwilligung**, vorzugsweise nach dem Prinzip des „Double-Opt-In"-Verfahrens, zum Schutz des Identitätsdiebstahls notwendig.
Stellensuchende	Für die Stellenbesetzung / allenfalls Aufnahme in Karriere-Pool	• Name des Verantwortlichen • Bearbeitungszweck • Empfänger der Daten und deren Ort (z.B. Software-Partner, Cloud-Dienstleister mit Sitz in der Schweiz) • Info, sofern über die Bewerbung automatisiert entschieden wird (KI) **Von der Art der Bewerbung unabhängig**, d.h. sowohl per Post, E-Mail, über öffentliches Jobportal, eigene Webseite, Softwaretool etc. **Einwilligung** für den Karriere-Pool notwendig.
Mitarbeitende	Zur Durchführung des Arbeitsvertrages und damit zusammenhängende gesetzliche Pflichten Überwiegende eigene Interessen	• Name des Verantwortlichen • Bearbeitungszweck • Empfänger der Daten und deren Ort (z.B. Software-Partner, Cloud-Dienstleister mit Sitz in der Schweiz) • Aufbewahrungsdauer **Aufnahme** ins Mitarbeiterreglement / Arbeitsvertrag / Weisung notwendig.
austretende Mitarbeitende / Rentner	Überwiegende eigene Interessen (Abwehr von Rechtansprüchen / Einhaltung eines Konkurrenzverbotes / Einfordern einer Konventionalstrafe) Gesetzliche Aufbewahrungspflichten	Die entsprechenden Personendaten dürfen solange aufbewahrt werden, wie sie für den Bearbeitungszweck notwendig sind. Bereits während dem Arbeitsverhältnis darauf hinweisen. **Löschfristen beachten!**

10. Vertraulichkeitsverpflichtung

Die Mitarbeitenden, welche mit Personendaten arbeiten, sind schriftlich zur Einhaltung der Vertraulichkeit und des Datenschutzes zu verpflichten. Das kann mit einer **Standardformulierung im Arbeitsvertrag** geschehen.

Darüber hinaus sind die **Mitarbeitenden** zu **schulen**! Nur wenn die Mitarbeitenden wissen und verstehen, wie sie mit Personendaten umgehen müssen und wo die Stolpersteine sind, können Datenpannen minimiert werden und das Datenschutz-Management-System funktioniert. Damit lassen sich Reputationsschäden sowie aufwendige Straf- und Verwaltungsmassnahmen vermeiden.

11. Einwilligung

Die Verwendung und Veröffentlichung von **fotografischen und / oder Bild- und Tonaufnahmen** sowie **Kontaktdaten** von Mitarbeitenden – soweit sie nicht in Erfüllung der arbeitsvertraglichen Pflicht offengelegt werden dürfen – bedürfen einer **Einwilligung der Mitarbeitenden**. Die Einwilligung muss **freiwillig** erfolgen.

Eine Einwilligung kann vom Mitarbeitenden jederzeit widerrufen werden. Ein **Widerruf** hat zur Folge, dass das Unternehmen ab diesem Zeitpunkt die Daten nicht mehr gemäss Einwilligung verwenden darf (Löschen auf Webseite etc.). **Wichtig ist dabei der Vorbehalt**, dass die Nutzung von bereits gedruckten Firmenbroschüren und -prospekten weiter möglich sein muss und dass bei Veröffentlichung im Internet durch die Nutzung von Dritten eine generelle Löschung nicht möglich ist.

12. Die Datenschutzbehörde der Schweiz

Der **Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB)** als Aufsichtsbehörde ist zuständig bei Datenbearbeitungen durch Bundesorgane und Private. Datenbearbeitungen durch kantonale und kommunale Behörden fallen **nicht** in seinen Zuständigkeitsbereich.

Die **Hauptaufgaben** des EDÖB sind:

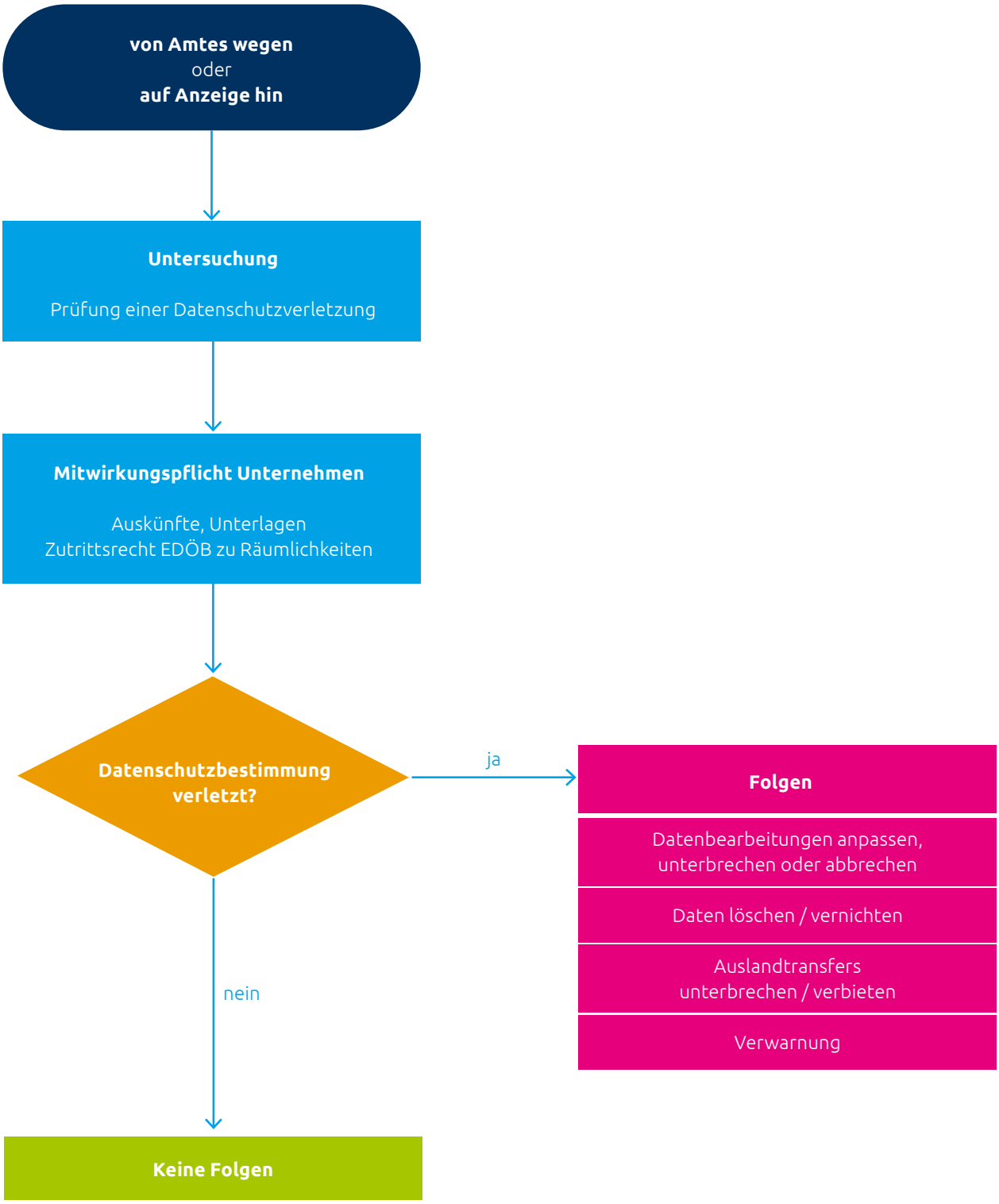
- **Beaufsichtigung** von Bundesbehörden und privaten Personen
- **Beratung** von Bundesbehörden, kantonalen Behörden und privaten Personen
- **Stellungnahme** zu Rechtsetzungsprojekten des Bundes
- **Schulung** von und **Informationen** an Bundesorgane und private Personen
- **Sensibilisierung** von und **Auskunft** an betroffene Personen
- Stellt **Arbeitsinstrumente** als Empfehlung zur Verfügung (Merkblätter, Leitfäden, Musterbriefe, abrufbar unter www.edoeb.admin.ch)
- **Zusammenarbeit** mit in- und ausländischen Datenschutzbehörden

13. Bussen und weitere Sanktionen

Das Datenschutzgesetz sieht verschiedene Möglichkeiten zur Durchsetzung der gesetzlichen Pflichten vor. Alle Massnahmen binden beim Unternehmen personelle Ressourcen. Dies führt zu **Kosten** und **Reputationsschäden**.

Verwaltungsmassnahmen

Der EDÖB kann **Verwaltungsmassnahmen** in Form von verbindlichen Verfügungen aussprechen. Die Untersuchung kann er von Amtes wegen einleiten oder wenn Dritte wie Mitarbeitende, Konkurrenten oder Website-Besucher bei ihm eine Anzeige erstatten. Das Vorgehen und die Folgen sehen für das Unternehmen wie folgt aus:

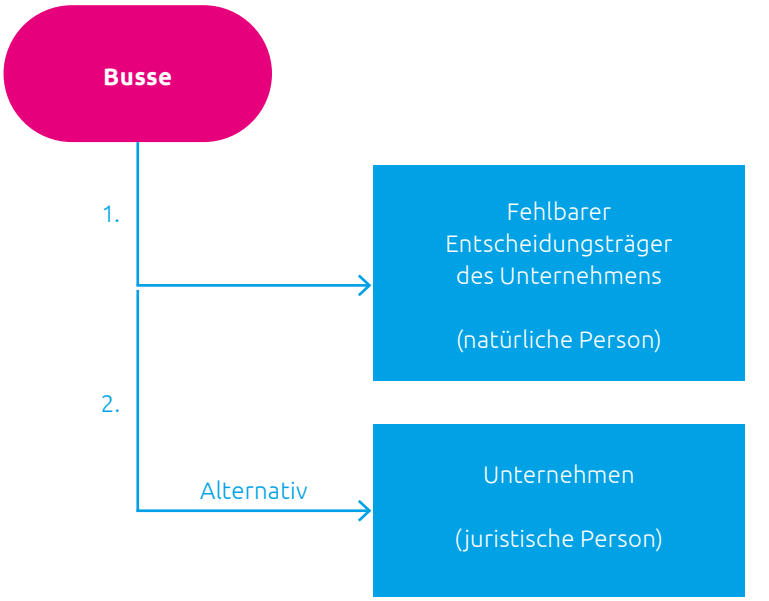


Strafrechtliche Massnahmen

Im Gegensatz zu den Aufsichtsbehörden gemäss DSGVO kann der EDÖB selber keine Bussen aussprechen. Die Verfolgung und Beurteilung von strafbaren Handlungen obliegt den Kantonen (Gerichte).

Auf **Antrag** wird mit **Busse von max. CHF 250 000** bestraft, wer **vorsätzlich** gegen die folgenden Pflichten verstösst:

Verletzungstatbestand	Beispiel
Verletzung der Informationspflicht	Betroffene werden gar nicht informiert.
Verletzung der Auskunftspflicht	Falsche oder unvollständige Auskunft **Nicht** bei keiner Auskunft **Empfehlung**: Nie den Eindruck erwecken, es wurden alle Personendaten gegeben.
Verletzung der Mitwirkungspflicht	Falsche Auskünfte an den EDÖB
Verletzung der Bestimmungen zum Datenexport	Datenbekanntgabe in einen unsicheren Drittstaat ohne geeignete Garantien.
Nicht konforme Beauftragung von Auftragsbearbeitern	Vertragliche Geheimhaltung verbietet eine Beauftragung.
Verletzung der Massnahmen zur Datensicherheit	Es bestehen keine aktuellen TOM.
Verletzung der beruflichen Schweigepflicht	Geheime Daten werden im Intranet aufgeschaltet.
Missachtung von Verfügungen des EDÖB oder der Beschwerdebehörde	Jedoch nur, wenn sie unter Strafandrohung nach Art. 292 StGB missachtet werden.



- Verwaltungsrat / Geschäftsführung
- Datenschutzberater
- HR-Verantwortlicher
- IT-Verantwortlicher

- Busse beträgt max. CHF 50 000
- Nur, wenn die Ermittlung des fehlbaren Entscheidungsträgers in einem unverhältnismässigen Aufwand zu Strafe steht.

Stand, Februar 2023

Balmer-Etienne AG
Luzern | Nidwalden | Zug | Zürich

info@balmer-etienne.ch
balmer-etienne.ch