Jardin Suisse
Unternehmerverband Gärtner Schweiz

JardinSuisse – Praxiswegleitung zum Datenschutz

Eine Übersicht und Hilfestellung zum Schweizer Datenschutzrecht für Mitglieder von JardinSuisse

Die Praxiswegleitung berücksichtigt das revidierte Bundesgesetz über den Datenschutz (in Kraft ab dem 01.09.2023; **DSG**). Wird vom DSG und seinen Vorgaben gesprochen, ist jeweils bereits das neue gemeint. Nicht Teil der Praxiswegleitung ist die Europäische Datenschutzgrundverordnung (**DSGVO**).

Diese Praxiswegleitung dient nur der Information und als Hilfestellung, sie stellt keine Rechtsberatung dar oder ersetzt eine solche. Die darin beschriebenen Grundsätze können im Einzelfall anders beurteilt werden. Die Nutzung erfolgt auf eigene Verantwortung. Jede Gewähr ist ausgeschlossen.

Inhaltsverzeichnis

I. EINLEITUNG

Kunden, Mitarbeitende und weitere Personen (z.B. Lieferanten und Dienstleister), deren Personendaten bearbeitet werden, erwarten einen verantwortungsvollen und rechtskonformen Umgang mit ihren Personendaten. Mit Blick auf die neue Gesetzeslage und das gesteigerte Bewusstsein in der Bevölkerung lohnt es sich, dem Datenschutz Beachtung zu schenken. Es sollen aber Prioritäten gesetzt werden – nicht alles ist gleich wichtig!

Die Grundsätze zur Datenbearbeitung haben sich mit der Revision des Datenschutzgesetzes nicht verändert. Datenbearbeitungen, die bisher zulässig waren, sind es auch unter dem neu-

en Recht. Die Neuerungen beinhalten einige zusätzliche Pflichten und ausgebaute Strafandrohungen.

II. BEGRIFFE

In diesem Abschnitt werden die wichtigsten Begriffe erläutert. Insbesondere «Personendaten» und «bearbeiten» haben eine breitere Bedeutung als auf den ersten Blick ersichtlich ist.

Begriff	Bedeutung
Was sind **Personendaten**?	Alle Informationen, die sich auf **bestimmte** oder **bestimmbare** Person beziehen, d.h. es ist ein Rückschluss auf die Identität anhand der Daten selbst oder mit entsprechenden Zusatzdaten möglich. Beispiele: • Personalien (Name, Geburtsdatum, etc.) • Kontaktdaten (Adresse, Telefonnummer, E-Mail, etc.) • physische Merkmale (Geschlecht, Augenfarbe, etc.) • Kennnummern (AHV-Nummer, etc.) • finanzielle Informationen (Kontonummer, Einkommen, etc.) • Standortdaten, IP-Adresse, Geräte-IDs • Nutzungs- / Verhaltensdaten, Präferenzen und Gewohnheiten
Was sind **besonders schützenswerte Personendaten**?	Bei den besonders schützenswerten Personendaten handelt es sich um Kategorien von Personendaten, für die das geltende Datenschutzrecht strengere Regeln vorsieht: • Daten über die Gesundheit oder die Intimsphäre • Daten über die Zugehörigkeit zu einer Rasse oder Ethnie • Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten • genetische Daten • biometrische Daten, die eine natürliche Person eindeutig identifizieren • Daten über Massnahmen der sozialen Hilfe • Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen
Tipp	Die Mitglieder von Jardin Suisse werden im Rahmen ihres Geschäfts bzw. bei der Abwicklung ihrer geschäftlichen Beziehungen und der Kundenverträge sehr selten bis gar nie besonders schützenswerte Personendaten bearbeiten. Wo aber besonders schützenswerte Personendaten anfallen können, ist im HR-Bereich (z.B. Informationen über Krankheiten oder Unfälle der Mitarbeiter, Einholung Strafregisterauszüge beim Bewerbungsverfahren etc.)
Was ist mit «**bearbeiten**» von Personendaten gemeint?	Damit ist jeder Vorgang im Zusammenhang mit den Personendaten gemeint (sowohl automatisierte als auch manuelle Vorgänge), d.h. alles, was mit Daten gemacht werden kann. Dazu gehören unter anderem (aber nicht abschliessend): das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.
Wer ist die «**be-**	Bei der betroffenen Person handelt es sich um die natürliche Person,

Begriff	Bedeutung
troffene Person»?	deren Personendaten bearbeitet werden. Das heisst der betroffene Kunde oder Kundin, Mitarbeitende oder weitere Personen, dessen bzw. deren Personendaten bearbeitet werden. Nicht darunter fallen juristische Personen wie z.B. Aktiengesellschaften.
Tipp	Die Bearbeitung von Daten von Unternehmen fällt im neuen Recht nicht mehr unter das Datenschutzgesetz. Bedenken Sie aber, dass wenn Sie Daten über Mitarbeitende von Unternehmen (z.B. Name einer Kontaktperson) bearbeiten, das Personendaten sind und damit das Datenschutzgesetz anwendbar ist.

III. WANN UND WIE DÜRFEN PERSONENDATEN BEARBEITET WERDEN?

A. Bearbeitungsgrundsätze

Die Bearbeitungsgrundsätze werden mit dem revidierten Datenschutzgesetz nicht geändert. Das bedeutet, dass Datenbearbeitungen, die bereits heute rechtmässig sind, dies auch weiterhin bleiben. In diesem Abschnitt finden Sie die Bearbeitungsgrundsätze kurz erläutert. Merken Sie sich insbesondere die 10 Leitsätze in den grünen Kästchen.

Rechtmässigkeit und Treu und Glauben	
Grundsatz	Die Bearbeitung muss rechtmässig, das heisst unter **Einhaltung der gesetzlichen Vorgaben** erfolgen und die Bearbeitung der Daten hat nach **Treu und Glauben** zu erfolgen. Es dürfen nur Personendaten bearbeitet werden, die nicht illegal (z.B. durch Ausspionieren) erhoben wurden.
Leitsatz I	Die Bearbeitung von Personendaten ist **grundsätzlich erlaubt**.
Leitsatz II	Das ist aber nur so, wenn • die **Bearbeitungsgrundsätze** eingehalten werden, • die betroffene Person der Bearbeitung **nicht widersprochen** hat und • keine besonders schützenswerten Personendaten an Dritte **bekannt gegeben** werden.
Leitsatz III	Bearbeiten Sie Daten fair, so wie Sie es auch selber erwarten würden (z.B. keine versteckten Überwachungskameras, kein heimlicher Verkauf der Daten).
Transparenz und Zweckbindung	
Grundsatz	**Transparenz** ist ein wichtiges Mittel, um Datenschutz zu betreiben: Es soll den betroffenen Personen immer klar sein, was mit ihren Daten wie gemacht wird und wem sie bekannt gegeben werden. Das schützt auch Ihr Unternehmen und hilft, Vertrauen zu schaffen.

	Transparenz bedingt insbesondere, dass die betroffenen Personen über die Datenbearbeitung **informiert** werden (siehe Kapitel IV.A.1). Personendaten dürfen zudem nur zu definierten **Zwecken** erhoben und bearbeitet werden, die bei der Beschaffung transparent angegeben werden oder die mit dem angegebenen Zweck vereinbar sind. Der Zweck kann sich auch aus den Umständen oder dem Gesetz ergeben.
Leitsatz IV	Informieren Sie in einer Datenschutzerklärung klar und offen darüber, welche Personendaten Sie erheben und für welche Zwecke Sie diese bearbeiten – und halten Sie sich daran.
Tipp	JardinSuisse stellt ihren Mitgliedern ein Muster zur Verfügung, welches die gängigsten Datenbearbeitungen der grünen Branche abdecken; Sie können dieses mit wenigen Anpassungen verwenden.
Verhältnismässigkeit	
Grundsatz	Das **Verhältnismässigkeitsprinzip** ist bei der Bearbeitung von Personendaten einzuhalten. Das verlangt insbesondere, dass • nur Daten erhoben und bearbeitet werden, die geeignet und erforderlich sind, um den verfolgten Zweck (wie er insbesondere in der Datenschutzerklärung dargelegt wird) zu erreichen (**Datensparsamkeit**); • Personendaten zu **löschen** oder zu **anonymisieren** sind, wenn sie **nicht mehr benötigt** werden und keine Aufbewahrungspflichten mehr bestehen; • innerhalb des Unternehmens die Mitarbeitenden nur auf jene Daten Zugriff erhalten, welche sie zur Erfüllung ihrer Arbeit benötigen ("**need-to-know**").
Beispiel	Ein Gartenbauunternehmen führt eine neue Software für die elektronische Archivierung ein. Der Geschäftsführer bestimmt, dass Dokumente, die in diese Software überführt werden, nicht mehr gelöscht werden dürfen, da er der Auffassung ist, dass sie irgendwann einmal nützlich sein könnten. Eine sozusagen unendliche Aufbewahrung von Dokumenten (die Personendaten enthalten) ist aber unverhältnismässig und verstösst daher gegen das Datenschutzgesetz. Personendaten dürfen nur so lange aufbewahrt werden, wie hierfür ein triftiger Grund besteht, also z.B. weil die Daten noch benötigt werden, um den Bearbeitungszweck zu erfüllen, weil eine Aufbewahrungspflicht besteht oder auch, weil die Daten als Beweismittel in einem laufenden oder zukünftigen Verfahren dienen.
Leitsatz V	Üben Sie sich in Datensparsamkeit und löschen oder anonymisie-

	ren (Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**) Sie die Daten, sobald Sie diese nicht mehr benötigen bzw. kein weiterer Grund für die Aufbewahrung gegeben ist.
Leitsatz VI	Die Datenablage und die Zugänge zu den Daten sollten so geregelt werden, dass die Mitarbeitenden nur auf die Daten Zugriff erhalten, welche sie für die Arbeit benötigen, nicht auf mehr.
Tipp	Hören Sie auf Ihr Bauchgefühl! Haben Sie das Gefühl, eine Datenbearbeitung könnte heikel sein, ist es häufig auch so. Finden Sie keine zuverlässige Antwort, lassen Sie sich von einem Spezialisten beraten.
Datenrichtigkeit	
Grundsatz	Unrichtige oder unvollständige Personendaten müssen **berichtigt** und **ergänzt** werden. Wer sich nicht sicher ist, ob Daten richtig sind, muss dies überprüfen. Geht das nicht, sind sie zu löschen bzw. die Zweifel sind zu vermerken. Die betroffene Person kann auch jederzeit eine Korrektur der eigenen Daten verlangen.
Leitsatz VII	Wenn Sie merken, dass benutzte Personendaten falsch oder unvollständig sind, korrigieren Sie dies. Wenn Sie unsicher sind, vermerken Sie dies, bis Sie sich Klarheit verschaffen konnten.
Persönlichkeits--verletzung	Werden die Grundsätze nicht eingehalten und besteht kein Rechtfertigungsgrund (siehe unten), führt dies zu einer ungerechtfertigten Persönlichkeitsverletzung der betroffenen Person und kann Schadenersatz auslösen.

B. Die Rechtfertigung – der "gute" Grund, Daten dennoch zu bearbeiten

Können die Grundsätze aus dem Leitsatz II nicht eingehalten werden, kann eine Bearbeitung dennoch zulässig sein, wenn ein Rechtfertigungsgrund vorliegt. Diese Rechtfertigungsgründe werden nachfolgend noch detaillierter erläutert.

1. Allgemein	
Leitsatz VIII	Kann der Leitsatz II nicht eingehalten werden, ist die Bearbeitung dennoch zulässig, wenn Sie einen guten Grund dafür haben (**Rechtfertigungsgrund).**

Mögliche Rechtfertigungsgründe	• **Einwilligung** durch die betroffene Person
	• Datenbearbeitung infolge einer **gesetzlichen Vorgabe**
	• **Überwiegendes privates oder öffentliches Interesse**, wie z.B. im Fall von
	  • Datenbearbeitungen in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages mit der betroffenen Person
	  • Datenbearbeitungen zur Prüfung der Kreditwür-

	digkeit, sofern gewisse zusätzliche Vorgaben eingehalten werden • Datenbearbeitungen zur Erstellung von anonymen Statistiken Weitere Rechtfertigungsgründe sind in Art. 31 DSG zu finden.
2. Einwilligung	
Voraussetzung	Eine Einwilligung ist nur gültig, wenn sie **informiert** und **freiwillig** erfolgt. • Informiert heisst, dass die betroffene Person darüber informiert wurde, für welche Daten und für welchen Zweck sie ihre Einwilligung erteilt (z.B. die Publikation eines spezifischen Fotos auf einer spezifischen Website). • Freiwillig ist die Einwilligung, wenn kein Druck ausgeübt wird.
Form	Eine Einwilligung kann auch mündlich erfolgen (keine Schriftlichkeit nötig). Zu Beweiszwecken empfiehlt es sich, die Einwilligung zu dokumentieren, z.B. durch • Schriftliche Einwilligung • Digitale Einwilligung durch Protokollierung einer Annahme
Widerruf	Einwilligungen können jederzeit widerrufen werden. Dies hat zur Folge, dass • jederzeit das Risiko besteht, die Daten in Zukunft nicht mehr bearbeiten zu dürfen. • die Umsetzung des Widerrufs sichergestellt werden muss.
Beispiel	• Sie müssen nicht die Einwilligung des Kunden abholen, damit Sie ihm wichtige Informationen über die Vertragsabwicklung per E-Mail (z.B. Auftragsbestätigung) senden dürfen. • Wenn Sie Ihren Kunden aber neu auch Werbung zustellen möchten (und Sie dies noch nie getan haben und auch nicht in Ihrer Datenschutzerklärung darüber informiert haben, dass Sie dies allenfalls tun können), dann benötigen Sie hierfür die Einwilligung des Kunden (da ein Verstoss des Zweckbindungsgrundsatzes vorliegt; siehe Kapitel III.A).
Leitsatz IX	Die Einwilligung ist kein "Allheilmittel". Stützen Sie sich daher nur dann auf die Einwilligung ab, wenn keine andere Möglichkeit zur Rechtfertigung der Datenbearbeitung besteht und diese sonst nicht zulässig wäre.
Tipp	Informieren Sie die betroffene Person, wie eine Einwilligung wider-

	rufen werden kann (z.B. per E-Mail, per Brief) und geben Sie eine Adresse an. Instruieren Sie Ihre Mitarbeitenden, ihnen gegenüber ausgesprochene Widerrufe an die richtige Stelle weiterzuleiten.
3. Gesetzliche Grundlage	
Grundsatz	Schreibt ein Gesetz die Datenbearbeitung oder Datenbekanntgabe vor, kann auch dies die Verletzung eines Bearbeitungsgrundsatzes rechtfertigen.
Beispiel	Eine Baumschule beschäftigt insgesamt fünf Mitarbeiter. Einer dieser Mitarbeiter ist mit seiner Stelle unzufrieden und fällt immer wieder mit negativen Äusserungen über die Baumschule auf. Als dieser Mitarbeiter erfährt, dass die Baumschule einmal im Jahr seinen Jahreslohn an die Pensionskasse, an der sie angeschlossen ist, übermittelt, ist er empört, denn er findet, der Lohn ist eine geheime Information, die niemanden etwas angeht. Er verlangt von der Baumschule, dass sie seinen Lohn ab jetzt nicht mehr an die Pensionskasse bekanntgibt (das ist ein "Widerspruch in die Datenbearbeitung", siehe Leitsatz II). Die Baumschule darf bzw. muss den Lohn trotz dieses Widerspruchs weiterhin an die Pensionskasse melden, da sie vom Gesetz über die berufliche Vorsorge (BVG) dazu verpflichtet wird (d.h. sie kann sich auf den Rechtfertigungsgrund der gesetzlichen Grundlage stützen). Denn nur so kann die Pensionskasse die Pensionskassen-Beiträge berechnen.

C. Datensicherheit

Grundsatz	Die Sicherheit der Personendaten muss jederzeit in angemessener Weise gewährleistet sein. Das bedeutet, es muss die • Vertraulichkeit (Schutz vor unbefugten Zugang/Zugriff) • Integrität (Schutz vor unberechtigter Manipulation) und • Verfügbarkeit (Schutz vor Verlust) der Daten sichergestellt werden. Das bedingt insbesondere, das Sie sicherstellen, dass Ihre IT-Infrastruktur auf dem neusten Stand ist, z.B. indem Sie vorgeschlagene Updates an Ihren Systemen zeitnah vornehmen und dass Sie Ihre Mitarbeitenden im Umgang mit der IT schulen. Auch die Datensicherheit muss, wie die oben aufgeführten Bearbeitungsgrundsätze, bei einer jeden Bearbeitung von Personendaten eingehalten werden. Seien Sie sich aber bewusst, dass eine Verletzung der Datensicherheit, anders als die Bearbeitungsgrundsätze, nicht gerechtfertigt werden. Auch kann die Verletzung der Datensicherheit strafrechtliche Folgen haben (unten), die Verletzung der Bearbeitungsgrundsätze hingegen nicht.

Leitsatz X	Achten Sie stets darauf, dass Personendaten bei Ihnen sicher sind.
Strafbarkeit	Mangelnde Datensicherheit kann strafbar sein. Nicht jede Datensicherheitsverletzung ist strafbar, aber der aktuelle technische Minimalstandard ist einzuhalten.
Tipp	Dies ist ein zentraler Punkt. Das Risiko für Personendaten ist bei mangelnder Datensicherheit viel grösser als z.B., wenn Daten etwas zu lange aufbewahrt werden. Packen Sie die Datensicherheit als einen der wichtigsten Punkte an.

IV. WAS MUSS DENN NUN GEMACHT WERDEN?

Nachfolgenden wird erläutert, welche Neuerungen das revidierte Datenschutzgesetz bringen wird. Das Kapitel gibt zudem Hilfestellung zur Umsetzung dieser neuen Pflichten im Unternehmen. Im Anhang der Wegleitung finden Sie auch eine Checkliste, in welcher Reihenfolge die Umsetzung in der Regel erfolgt.

A. Dokumentations- und Informationspflichten

1. Datenschutzerklärung (DSE)	
Wieso muss das gemacht werden?	Das DSG sieht vor, dass über gewisse Aspekte der Datenbearbeitung aktiv informiert werden muss; das ist Teil der verlangten Transparenz (siehe Kapitel III.A). Dies erfolgt mit der **Datenschutzerklärung (DSE)**.
Über was muss informiert werden?	Eine DSE sollte folgende Inhalte aufweisen: • Die **Identität** und die Kontaktdaten der Verantwortlichen. Damit ist das verantwortliche Unternehmen gemeint. Es muss keine Person aufgeführt werden. • Den **Bearbeitungszweck**. Führen Sie aus, für welche Zwecke Sie Daten bearbeiten (z.B. Kommunikation, Abwicklung von Verträgen) • Die **Empfängerinnen** und **Empfänger** oder die **Kategorien von Empfängerinnen und Empfängern**, denen Personendaten bekanntgegeben werden • Werden Personendaten nicht direkt bei der betroffenen Person beschafft, so sind ihr zudem die **Kategorien der bearbeiteten Personendaten** mitzuteilen. • Werden Personendaten ins Ausland bekannt gegeben, so ist auch über die **Staaten**, in welche Daten bekannt gegeben werden, und allenfalls über die Verwendung von zusätzlichen **Schutzmassnahmen** zu informieren.
Was ist zu beachten?	• Die DSE sollte über alle Datenbearbeitungen informieren. Häufig werden in Datenschutzerklärungen nur die Bearbeitungen im Zusammenhang mit der Website abgedeckt, was unzureichend ist. Nennen Sie alle Bearbeitungen, wie z.B. Marketing, Buchhaltung, Auftragsabwicklung, etc. • Die DSE sollte einfach auffindbar sein (z.B. Fussbereich der Website). • Die DSE soll nicht akzeptiert oder Teil des Vertrages werden • Weisen Sie hingegen z.B. in Verträgen auf ihre DSE hin und sagen Sie, wo diese zu finden ist. *Formulierungsvorschlag: «Die Bearbeitung von Personendaten ist in unserer Datenschutzerklärung beschrieben, die wir unter [LINK] bereithalten.»*

	• Eine DSE sollte jederzeit aktuell sein und kann jederzeit geändert werden.
Strafbarkeit	Fehlt die Datenschutzerklärung oder ist der Mindestinhalt nicht abgedeckt (z.B. nur Bearbeitungen auf der Website), kann dies mit Busse bestraft werden.
Tipp	Die Datenschutzerklärung gehört zum Ersten, was Sie in Angriff nehmen sollten. Dies, da das Fehlen einerseits strafbedroht und anderseits sofort ersichtlich ist.
Tipp	Ist die DSGVO nicht anwendbar (siehe VII), sollte nicht eine Datenschutzerklärung nach DSGVO-Muster erstellt werden. Die Mindestangaben gemäss dem revidierten DSG ähneln sehr stark den Anforderungen der DSGVO, sie sind jedoch nicht komplett deckungsgleich und in einem Punkt ist das revidierte DSG sogar strenger als die DSGVO. Verlassen Sie sich daher nicht auf DSGVO-Muster. Vermeiden Sie insbesondere die Aussage, dass Sie die DSGVO einhalten. Falls die DSGVO anwendbar ist (siehe VII), sind weitergehende Inhalte vorgeschrieben. Sie finden ein sehr umfassendes Muster für eine DSGVO-Datenschutzerklärung (die aber auch das revidierte DSG abgedeckt) unter www.dsat.ch
Tipp	JardinSuisse stellt ein Muster einer Datenschutzerklärung zur Verfügung.
2. Das Bearbeitungsverzeichnis	
Wieso muss das gemacht werden?	Das Bearbeitungsverzeichnis gibt einen Überblick über die im Unternehmen vorhandenen Bearbeitungstätigkeiten. Ein solcher Überblick ist notwendig, damit der Datenschutz überhaupt systematisch im Unternehmen umgesetzt werden kann.
Wer muss ein Bearbeitungsverzeichnis führen?	Grundsätzlich muss jedes Unternehmen ein Bearbeitungsverzeichnis stellen. Ausgenommen sind Unternehmen mit weniger als 250 Mitarbeitenden (wobei auch hier wiederum Ausnahmen bestehen).
Tipp	Mitglieder von JardinSuisse werden häufig unter die Ausnahme von weniger als 250 Mitglieder fallen. Allerdings ist es auch für diese empfehlenswert ein Verzeichnis zu erstellen. Dieses kann weniger detailliert sein, ist aber notwendig, um sich einen Überblick über die bestehenden Datenbearbeitungen zu verschaffen und hilft dadurch z.B. die Datenschutzerklärung zu erstellen.
Tipp	Ein Verzeichnis kann z.B. in Excel geführt werden.
3. Datenschutz-Folgenabschätzung (DSFA)	
Wann ist eine DSFA nötig?	Ist eine geplante Datenbearbeitung für die betroffene Person möglicherweise risikoreicher, muss eine Datenschutz-Folgenabschätzung (**DSFA**) erstellt werden.

Was ist eine DSFA?	Darin werden das das Vorhaben und die Massnahmen zum Schutz der betroffenen Person dokumentiert und es wird geprüft, ob trotz der Massnahmen hohe Risiken unerwünschter negativer Folgen für die betroffene Person bleiben. Eine DSFA kann beispielsweise bei der Einführung einer Videoüberwachung nötig sein.
Tipp	Die Mitglieder der grünen Branche werden nur selten tatsächlich eine DSFA durchführen müssen. Ein vom Gesetz vorgesehener Fall, der häufig zur Anwendung gelangt, wäre z.B., wenn öffentliche Bereiche (z.B. Parkplatz, Verkaufsfläche etc.) per Video überwacht werden. Wenn Ihr Unternehmen dies tut, führen Sie eine DSFA durch. Holen Sie sich hierfür allenfalls Unterstützung.

B. Die Nutzung von Dienstleistern

1. Auftragsbearbeitung	
Was ist eine Auftragsbearbeitung?	Wenn Ihr Unternehmen einen Dritten (**Auftragsbearbeiter**) für eine eigene Datenbearbeitung hinzuzieht (z.B. Hosting-Anbieter, Cloudprovider), bleibt dennoch Ihr Unternehmen für die Datenbearbeitung verantwortlich (das Unternehmen wird entsprechend der **Verantwortliche** genannt). Die Bearbeitung erfolgt im Interesse des Unternehmens und dieses entscheidet über die Art und Weise der Bearbeitung. Ein Auftragsbearbeiter bearbeitet die Daten nur auf Weisung und im Auftrag des oder der Verantwortlichen.
Was muss berücksichtigt werden?	Das DSG schreibt vor, dass in solchen Fällen ein Vertrag zwischen dem Verantwortlichen und dem Auftragsbearbeiter abgeschlossen werden muss (Auftragsbearbeitungsvertrag, oder auch Auftragsdatenverarbeitungsvertrag [ADV] oder Data Processing Agreement [DPA] genannt). Dies erfolgt häufig in einem Anhang oder einem separatem Vertrag, welcher zum eigentlichen Auftrag (Hauptvertrag) hinzukommt.
Was sollte in diesem Vertrag enthalten sein?	Das DSG sieht keine Liste von zwingenden Inhalten vor. Die folgenden Punkte stellen jedoch die üblichen Inhalte dar, welche auf jeden Fall in einem solchen Vertrag enthalten sein sollten. • Vertragsparteien • Gegenstand und Dauer der Bearbeitung • Zweck der Bearbeitung • Ort der Bearbeitung und Regelung über den Datentransfer ins Ausland (Unter welchen Bedingungen ist die Bekanntgabe ins Ausland erlaubt?). • Kategorien der betroffenen Personen und der bearbeiteten Personendaten. • Verpflichtung die Daten vertraulich zu behandeln. • Pflicht des Auftragsbearbeiters Verletzungen der Datensicherheit zu melden. • Pflicht des Auftragsbearbeiters nur aufgrund dokumen-

	tierter Weisung des Verantwortlichen Daten zu bearbeiten • Recht des oder der Verantwortlichen, die Datenbearbeitung zu prüfen • Pflicht des Auftragsbearbeiters oder der Auftragsbearbeiterin, die Datensicherheit zu gewährleisten (technische und organisatorische Massnahmen [TOMs]) • Pflicht des Auftragsbearbeiters oder der Auftragsbearbeiterin, die Daten zurückzugeben und zu löschen • Der Beizug von Dritten durch den Auftragsbearbeiter oder die Auftragsbearbeiterin sollte geregelt sein • Unterstützungspflichten des Auftragsbearbeiters oder der Auftragsbearbeiterin bei der Einhaltung des DSG.
Strafbarkeit	Das Hinzuziehen eines Auftragsbearbeiters ohne einen rechtskonformen Vertrag kann bestraft werden.
Tipp	Prüfen Sie Ihre Verträge mit Dienstleistern und achten Sie darauf, ob so ein Vertrag abgeschlossen wurde.
Tipp	Viele Dienstleister haben mittlerweile eigene Standard-ADV – fragen Sie am besten einfach nach.
Tipp	Ein ADV nach der DSGVO genügt grundsätzlich auch in der Schweiz, sollte aber auch die Einhaltung des Schweizer Rechts zusichern (das muss explizit im Vertrag stehen).
2. Datenbekanntgabe ins Ausland	
Wann dürfen Daten ins Ausland bekannt gegeben werden?	Daten dürfen ins Ausland bekannt gegeben werden, wenn entweder • das Land über angemessenen Datenschutz verfügt (z.B. EWR, nicht USA) *oder* • zusätzliche Schutzmassnahmen wie vertragliche Vereinbarungen (Standardvertragsklauseln) getroffen wurden *oder* • eine Ausnahme vorliegt (z.B. Einwilligung)
Strafbarkeit	Werden Daten in ein Land bekannt gegeben, ohne die oben genannten Voraussetzungen zu erfüllen, kann dies strafbar sein.
Tipp	Wenn Sie die Verträge mit Ihren Dienstleistern prüfen, prüfen Sie auch gleich, ob Ihre Daten ins Ausland gehen. Es kann zwar sein, dass die Daten auf Servern im EWR oder der Schweiz liegen, dass der Dienstleister aber im Ausland sitzt (z.B. USA) und unter bestimmten Bedingungen auf die Daten zugreift – auch ein solcher Fernzugriff ist eine Bekanntgabe ins Ausland. Der Begriff der «Bekanntgabe» ist somit weiter, als er vielleicht anfänglich vermuten lässt. Es ist auch möglich, dass nicht Sie direkt, aber Ihr Dienstleister Daten ins Ausland bekannt gibt. Wenn das der Fall ist, lassen Sie sich

	zusichern, dass er die notwendigen gesetzlichen Anforderungen einhält.
Tipp	Werden Daten in ein Land ohne angemessenen Datenschutz bekannt gegeben, kann es sinnvoll sein, Beratung hinzuzuziehen (für Cloud siehe Kapitel IV.B.3).
Tipp	Der Bundesrat legt nach dem neuen Recht die Länder mit angemessenem Datenschutz fest. Diese sind im Anhang zur Datenschutzverordnung zu finden.
3. Die Nutzung der Cloud	
Cloud	Viele Angebote und Software-Lösungen können nur noch aus der Cloud bezogen werden. Die Nutzung solcher geschäftlicher Cloud-Lösungen ist grundsätzlich möglich, es sind aber ein paar Faustregeln zu beachten. Datenschützende kritisieren die Cloud hingegen häufig, vor allem wegen den USA.
Tipp	Die folgenden Faustregeln sollten bei Cloud-Lösungen berücksichtigt werden: • Keine Nutzung von Diensten für Private zu geschäftlichen Zwecken (z.B. Hotmail, Dropbox für Private, Gmail). • Wählen Sie einen Provider mit Sitz im EWR oder der Schweiz und mit Speicherung der Daten im EWR oder der Schweiz. Das kann auch ein europäisches Tochterunternehmen eines Providers aus den USA sein. • Schliessen Sie mit dem Provider einen Auftragsbearbeitungsvertrag ab • Aktivieren Sie im Falle von besonders heiklen Daten, wenn möglich die Option, dass der Provider vor einem Datenzugriff fragen muss. • Verstehen Sie, wie ein Cloud-Dienst sicher zu konfigurieren ist. • Sichern Sie die Daten ausserhalb der Cloud (Provider sichern nicht). • Haben Sie einen Plan für den Fall, dass die Cloud ausfällt oder vom Provider innert kurzer Frist wegmigriert werden muss.

C. Betroffenenrechte

1. Auskunftsrecht	
Grundsatz	Betroffene Personen haben das Recht, Auskunft über eine Datenbearbeitung zu erhalten.
Auskunft	Ein Auskunftsgesuch muss innert 30 Tagen beantwortet werden. Die Beantwortung muss grundsätzlich kostenlos erfolgen. Auskünfte können teilweise oder vollständig verweigert werden, z.B.

	zum • Schutz von anderen Personen (mit einer Auskunft dürfen keine Personendaten anderer bekanntgegeben werden.) • Schutz von Geschäftsgeheimnissen
Umsetzung	Kleinere Unternehmen und/oder wenn kaum Gesuche erwartet werden: • Bestimmung einer zuständigen Person (z.B. die Datenschutzperson) • Diese muss sich im Falle eines Gesuchs darum kümmern (Achtung Frist) und allenfalls einen Spezialisten oder eine Spezialistin zur Unterstützung beiziehen • Alle Mitarbeitenden instruieren (z.B. mit Datenschutzweisung), dass solche Anfragen an die Datenschutzperson weitergeleitet werden sollen Grössere Unternehmen und/oder wenn viele Gesuche erwartet werden: • Definition eines Prozesses • allenfalls Erlass einer Weisung
Strafbarkeit	Eine vorsätzlich falsche oder unvollständige Auskunft kann bestraft werden.
Tipp	Bestätigen Sie nie die Vollständigkeit einer Auskunft (das kann selten wirklich mit Sicherheit gesagt werden), auch wenn dies der Gesuchsteller verlangt. Lassen Sie sich bei Unsicherheit beraten.
Tipp	Wichtig ist sicherzustellen, dass wenn ein solches Begehren eingeht, es umgehend bearbeitet wird und es nicht liegen bleibt. 30 Tage sind schnell vorbei.
2. Berichtigungs- und Löschrecht	
Grundsatz	Betroffene Personen haben das Recht, unrichtige Personendaten korrigieren zu lassen. Sie hat zudem das Recht zu verlangen, dass Ihre Daten gelöscht werden.
Umsetzung	Siehe Kapitel IV.C.1 zum Auskunftsrecht.
3. Weiteres zur Datenlöschung	
Welche Daten dürfen (allenfalls trotz Löschbegehren) aufbewahrt werden?	• Daten für notwendige Geschäftszwecke, das heisst Daten, die zur Erfüllung der Aufgabe (z.B. Vertragserfüllung oder Arbeitsverhältnis) notwendig sind • Daten, die nicht zwingend für den Geschäftszweck sind, mit deren Bearbeitung aber ein legitimer Zweck verfolgt wird, wie z.B. Daten für Marketing oder zu Dokumentationszwecken • Daten, für welche gesetzliche Aufbewahrungspflichten bestehen, wie z.B. bei der Buchhaltung oder im Steuerbereich

Wann müssen Daten gelöscht werden?	Wenn eine betroffene Person die Löschung Ihrer Daten verlangt, wenn nicht weiterhin ein Grund für die weitere Aufbewahrung besteht (siehe oben). Das Unternehmen muss aber bereits von sich aus die Personendaten löschen oder anonymisieren, sobald sie für den Zweck der Bearbeitung nicht mehr erforderlich sind. Besteht kein solcher Zweck mehr und ist eine allfällige Aufbewahrungspflicht abgelaufen und bestehen auch sonst keine Rechtfertigungsgründe für die weitere Aufbewahrung, müssen Daten gelöscht oder anonymisiert werden. Die allenfalls anwendbaren Aufbewahrungsfristen können sehr unterschiedlich ausfallen. So z.B. • Geschäftsbücher und Buchungsbelege 10 bis 15 Jahre • Daten von abgewiesenen Bewerbern nur kurze Zeit (maximal ein paar Wochen nach der Absage)
Umsetzung der Datenlöschung	Die Löschpflichten können manuell oder automatisiert umgesetzt werden, wobei in der Praxis häufig eine Mischform davon zur Anwendung kommt. Eine vollständige Anonymisierung ist der Löschung (aus datenschutzrechtlicher Sicht) gleichzusetzen.
Tipp	Gehen Sie mit der Information, etwas sei "anonymisiert" vorsichtig um. Eine Anonymisierung ist nur dann gegeben (und kann damit einer Löschung gleichgestellt werden), wenn eine Re-Identifikation praktisch ausgeschlossen werden kann bzw. diese nur mit einem übermässigen Aufwand noch möglich wäre. Das ist aufgrund der immer grösseren Datenmengen, die bearbeitet werden, häufig nicht mehr der Fall.
Aufbewahrungsrichtlinie und Umsetzung	Die Umsetzung der Löschung erfolgt gewöhnlich innerhalb einer Aufbewahrungsrichtlinie, welche bestimmt, wie lange Daten aufzubewahren und wie sie zu löschen sind. Gehen Sie Ihre Datenbestände durch und legen Sie für alle fest, wie lange die Daten aufbewahrt werden sollen. Nebst den gesetzlichen Fristen zählt auch, wie lange Sie Daten für Beweiszwecke brauchen. Dann bestimmen Sie jemanden, der oder die den jeweiligen Datenbestand regelmässig bereinigen muss, oder führen Sie z.B. jedes Quartal zusammen eine Aufräumaktion durch.

D. Meldepflicht bei Datensicherheitsverletzungen

Was muss gemeldet werden?	Verletzungen der Datensicherheit (z.B. Hackerangriff, unabsichtliche Veröffentlichung von Personendaten) müssen so rasch als möglich dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten gemeldet werden. Das heisst aber nicht, dass jede Verletzung gemeldet werden muss, sondern nur solche, die zu einem hohen Risiko für betroffene Personen führen.

Beispiel	Der Versand einer vertraulichen E-Mail an eine falsche Person muss nicht gemeldet werden. Ein Hackerangriff, der zur Veröffentlichung sämtlicher Daten der Kunden eines Unternehmens führt, muss vermutlich gemeldet werden.
Tipp	Überlegen Sie sich, wie Sie mit allfälligen Sicherheitsverstössen umgehen möchten, auch wenn Ihr Unternehmen noch nie mit einem solchen konfrontiert war. Sie müssen keinen umfassenden Prozess aufsetzen, aber definieren Sie die Verantwortlichkeiten, damit im Ernstfall möglichst rasch gehandelt werden kann.
Tipp	Ziehen Sie im Falle einer grösseren Datensicherheitsverletzung umgehend (auch am Wochenende) technische Unterstützung von IT-Spezialisten bei, um die Datensicherheit wiederherzustellen. Ziehen Sie ebenfalls umgehend und noch vor einer allfälligen Meldung an den EDÖB juristische Beratung bei.

E. Schärfung des "Datenschutzbewusstseins"

Weisungen / Anleitungen	Auch wenn das Gesetz keine ausdrückliche Pflicht kennt, eine Datenschutzweisung zu erlassen, sollten die Mitarbeitenden (auch bei kleinen Unternehmen) zumindest über den Umgang mit Personendaten instruiert sein. Kommt es zu einem Verstoss, wird das sonst der Leitung (Verwaltungsrat, Geschäftsleitung, Geschäftsinhaber) vorgeworfen. Es sollte zumindest eine kurze Weisung / Anleitung geben, wie mit Personendaten umgegangen werden soll und an wen man sich bei Fragen wenden soll. In grösseren Unternehmen können darin auch genauere Verantwortlichkeiten und Prozesse dokumentiert werden.
Tipp	Die wichtigsten Punkte des Datenschutzrechtes für KMUs auf einer Seite sind unter den folgenden Links zu finden. Dieser Survival Guide kann auch gleich als **Kurz-Weisung** im Unternehmen für den Umgang mit Personendaten erlassen werden. Darauf können zudem die Datenschutzperson und weitere Kontakte eingetragen werden. Dies ist das Minimum, was ein Unternehmen haben sollte. Link: Deutsch, Französisch, Englisch
Schulungen und Anleitungen	Die Mitarbeitenden sollten im Umgang mit Personendaten und der Informationssicherheit (z.B. Phishing) geschult werden.

V. WER MUSS DAS DENN NUN IN UNSEREM UNTERNEHMEN MACHEN?

Datenschutzperson oder Datenschutzstelle (dies ist keine offizielle Bezeichnung, die Bezeichnung kann	Es ist hilfreich und empfehlenswert, im Unternehmen jemanden zu bestimmen, der sich um den Datenschutz kümmern soll (**Datenschutzperson**). Dabei handelt es sich in der Regel nicht um einen Datenschutzberater oder um den Datenschutzbeauftragten, wie die Funktion teilweise auch genannt wird. Es ist keine Pflicht, so jeman-

auch anders lauten)	den zu bestimmen, es hilft aber, wenn jemand sich um die Umsetzung des Datenschutzes kümmert.
	• Das können die Geschäftsinhabenden persönlich, jemand aus dem Leitungsteam oder sonst interessierte Mitarbeitende sein. Je grösser das Unternehmen ist, desto mehr Kapazität muss für die Umsetzung eingerechnet werden und es ist unter Umständen eine eigene Stelle dafür zu schaffen (**Datenschutzstelle**).
	• Das heisst nicht, dass diese Person für die Datenbearbeitungen im Unternehmen verantwortlich ist, diese Verantwortung kann nicht einfach auf jemanden übertragen werden. Vielmehr verbleibt die Verantwortung für die Datenbearbeitungen an sich jeweils bei der Person, die im Alltag über die Ausgestaltung der Datenbearbeitung entscheidet (z.B. über den Einsatz einer Software) oder bei der Geschäftsleitung (Verwaltungsrat etc.), welche die Gesamtverantwortung trägt und die Rahmenbedingungen setzen muss (siehe Strafbarkeit Kapitel VII).
	• Die Aufgaben der Datenschutzperson können sein
	  • Die Umsetzung des Datenschutzes voranzutreiben
	  • Datenschutzerklärung zu erstellen (bzw. die Erstellung in Auftrag zu geben und zu begleiten)
	  • Mitarbeitende zu schulen und ein Bewusstsein für den Datenschutz im Unternehmen zu fördern
	  • Ansprechperson für Fragen von Mitarbeitenden zu sein
	  • Anfragen betroffener Personen zu beantworten (siehe IV.C.1)
	  • Widerrufe von Einwilligungen entgegenzunehmen
	  • Rechtskonformität von Bearbeitungen zu prüfen und "Alarm" zu schlagen, wenn etwas heikel sein sollte
	  • Verträge bezüglich Datenschutzes zu prüfen (Auftragsbearbeitung siehe IV.B.1)
	  • Zu wissen wo Unterstützung geholt werden kann (externe Spezialisten), wenn nötig
	• Voraussetzungen
	  • Es sollten das Interesse und die Kapazität vorhanden sein.
	  • Das Grundwissen kann mit dieser Wegleitung, Seminaren/Referaten und dem Internet aufgebaut werden.
	• In komplexeren Fällen oder bei Unklarheiten ist eine Beratung hinzuzuziehen.

Datenschutzberater	Schweizer Unternehmen können einen Datenschutzberater benennen. Dies ist aber für Private nicht verpflichtend.

VI. KLEINER EXKURS: BEARBEITUNG VON DATEN ÜBER ARBEITNEHMENDE

In diesem Kapitel werden einige Hinweise zur Bearbeitung von Daten über Arbeitnehmende gegeben.

Grundsatz	Der Arbeitgeber darf Daten des Arbeitnehmenden bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Das heisst: • Daten, welche sich auf die Beurteilung der **Eignung** des oder der betreffenden Arbeitnehmenden für eine Stelle oder eine Aufgabe im Arbeitsverhältnis beziehen (z.B. Lebenslauf, Zeugnisse) • Daten, die für die **Erfüllung der gesetzlichen und arbeitsvertraglichen Pflichten** notwendig sind (z.B. Lohnzahlen, Versicherungen, Unfallmeldungen) • Daten, die im Rahmen der Arbeitsleistung entstehen oder **zur Erfüllung der Arbeitsleistung notwendig** sind (z.B. E-Mails) Zusätzlich sind die Bearbeitungsgrundsätze in Kapitel III.A zu beachten.
Informationspflichten	• Arbeitnehmende müssen nicht über Datenbearbeitungen informiert werden, die gesetzlich notwendig sind. Dies beinhaltet die üblichen Datenbearbeitungen welche für das Arbeitsverhältnis notwendig sind wie z.B. Lohnzahlungen oder Unfallmeldungen. • Darüberhinausgehende Bearbeitungen (z.B. Überwachungsmassnahmen wie Videoüberwachungen oder Überwachung der Internetnutzung) müssen transparent kommuniziert werden (Datenschutzerklärung für Arbeitnehmende).
Rechtfertigung	• Möchte der Arbeitgeber über den Grundsatz (siehe oben) hinaus Daten bearbeiten, dann benötigt er hierfür einen Rechtfertigungsgrund (siehe Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**). • Das Subordinationsverhältnis führt zu erhöhten Anforderungen an die Freiwilligkeit bei Einwilligungen von Arbeitnehmenden. Eine Einwilligung ist gültig, wenn sie informiert und ohne Druck und Befürchtung von Nachteilen erfolgt ist.
Beispiele	• Die Veröffentlichung von Fotos von Arbeitnehmenden auf der Website benötigt grundsätzlich eine Einwilligung. Der Arbeitnehmende darf nicht unter Druck gesetzt werden, einzuwilligen (z.B. durch berufliche Nachteile). • Gehört die Veröffentlichung eines Profilbildes zur Stelle dazu (z.B. bei Leitungspositionen, Geschäftsführung), ist hingegen keine Einwilligung nötig. • Ein Team-Geburtstagskalender setzt in der Regel eine Einwilligung voraus (nicht nötig für die Arbeit). Der Jahrgang ist wegzulassen, da für die Erfüllung des Zwecks (nämlich damit

	die Teammitglieder wissen, wann sie wem zum Geburtstag gratulieren können) nicht notwendig (Datensparsamkeit).

VII. UND ZULETZT: IST DIE EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG (DSGVO) FÜR UNS ANWENDBAR?

Für Schweizer Unternehmen	Für Schweizer Unternehmen ist die DSGVO nur anwendbar, wenn das Unternehmen • an natürliche Personen im europäischen Wirtschaftsraum (EWR) **Waren oder Dienstleistungen** anbietet, oder • das **Verhalten** von natürlichen Personen im EWR **beobachtet**. Für die Mitglieder der grünen Branche in der Schweiz wird die DSGVO in der Regel nicht anwendbar sein, ausser sie richten ihr Angebot explizit auch auf Personen im EWR (z.B. im Fürstentum Liechtenstein) aus, z.B. indem sie im EWR aktiv Werbung machen.
Tipp	Entgegen dem, was man immer wieder hört, fällt ein Unternehmen nicht bereits unter die DSGVO, nur, weil es einen Grenzgänger aus dem EWR beschäftigt oder weil z.B. der Provider, der die Website hostet, sich im EWR befindet oder weil die Website auch aus dem EWR zugänglich ist. Entscheidend sind allein die oben genannten Punkte.
Tipp	Wenn Sie Tracking-Tools auf Ihrer Website einsetzen und damit auch das Verhalten von Nutzern aus dem EWR auf Ihrer Website tracken, dann KANN (muss aber nicht) das eine Verhaltensbeobachtung darstellen und die Anwendbarkeit der DSGVO auslösen. Damit der Einsatz von Tracking-Tools als Verhaltensbeobachtung gilt, müssen die folgenden Voraussetzungen gegeben sein: • es werden umfassende Angaben gesammelt, wodurch ein Profil über die Nutzer entstehen könnte; • die Nutzer, deren Verhalten auf der Website aufgezeichnet wird, befinden sich (zumindest teilweise) im EWR; • die Aktivitätsdaten gesammelt werden, um das individuelle Verhalten der Personen zu analysieren. Der Einsatz "nur" von Google Analytics reicht da regelmässig nicht. Hilfsmittel: • VISCHER-Tracking-Checklist: https://www.rosenthal.ch/downloads/VISCHER-Tracking-Checklist.pdf • Google Analytics: How to legally use Google Analytics in Europe - 7 March 2022 - VISCHER Als einfache Lösung können aber auch eine Zustimmungs-/Ablehnungslösung in der Schweiz eingesetzt werden oder die IP-

	Adressen aus dem EWR vom Tracking ausgefiltert werden
Tipp	Unter www.dsat.ch finden Sie eine ausführliche Checkliste, um die Anwendbarkeit der DSGVO auf Ihr Unternehmen zu prüfen (DSAT.ch Formular C.1 Anwendbares Recht – Ermittlung des relevanten Datenschutzrechts)
Fürstentum Liechtenstein	Das Fürstentum Liechtenstein ist Mitglied des EWR und die DSGVO ist auf Unternehmen im Fürstentum Lichtenstein anwendbar.
Tipp	Die Datenschutzstelle Fürstentum Liechtenstein hat viele Informationen und Angebote auf ihrer Website publiziert: www.datenschutzstelle.li

VIII. STRAFBARKEIT

Mit dem revidierten DSG werden die Strafbestimmungen ausgeweitet und die Bussen erhöht.

1. Allgemeines	
Wen trifft die Strafe?	Die Strafbestimmungen des DSG treffen – im Gegensatz zu der DSGVO – nicht das Unternehmen, sondern die dafür verantwortliche natürliche Person. • Diejenige Person, die die Verletzung begangen hat (z.B. ein Geheimnis verraten hat; die entschieden hat, einen Auftragsbearbeiter oder eine Auftragsbearbeiterin ohne entsprechenden Vertrag einzusetzen oder Daten ins Ausland bekannt zu geben, ohne die Vorgaben einzuhalten) • Die Datenschutzperson ist es in der Regel nicht, ausser sie ist für etwas ausdrücklich zuständig und diejenige die entscheidet (z.B. die Datenschutzperson ist für die Bearbeitung eines Auskunftsgesuchs verantwortlich und gibt vorsätzlich eine falsche Auskunft) • Der Verwaltungsrat, die Geschäftsführung, die Inhabenden, etc. Das heisst die Stelle, welche die Oberaufsicht über das Unternehmen hat, die entsprechenden Entscheide trifft und auch darüber entscheidet, ob entsprechende Weisungen erlassen werden und Ressourcen zur Verfügung gestellt werden
Wie hoch ist die Strafe?	• Busse von bis zu CHF 250'000.– • Die Busse kann nicht vom Arbeitgeber oder der Arbeitgeberin übernommen werden und ist nicht versicherbar
Was ist strafbar?	Die vorsätzliche Verletzung der nachfolgenden Vorgaben ist strafbar. Die fahrlässige Verletzung ist nicht strafbar. Aber der sogenannte Eventualvorsatz (das heisst, es wurde «in Kauf genommen») fällt auch unter Vorsatz. • Verletzung von Informationspflichten (z.B. keine oder nur eine ungenügende Datenschutzerklärung) (siehe Kapitel IV.A.1)

	• Verletzung von Auskunftspflichten (siehe Kapitel IV.C.1) • Bekanntgabe von Personendaten in Länder ohne ein angemessenes Datenschutzniveau, ohne das Treffen zusätzlicher Schutzmassnahmen oder ohne dass eine Ausnahme einschlägig ist (siehe Kapitel IV.B.2) • Kein Vertrag mit Auftragsbearbeiter (siehe Kapitel IV.B.1) • Verletzung der Datensicherheit: nicht jede Verletzung ist strafbar, aber der angemessene Standard ist einzuhalten (siehe Kapitel III.A**Fehler! Verweisquelle konnte nicht gefunden werden.**) • Verletzung des «kleinen Berufsgeheimnisses» (siehe unten Kapitel VIII.2)
2. «Kleines Berufsgeheimnis»	
Strafbarkeit	Wer geheime Personendaten, die sie oder er im Rahmen der Ausübung der beruflichen Tätigkeit anvertraut erhalten hat (z.B. Gesundheitsdaten der Kinder) einem oder einer Unberechtigten bekannt gibt, kann mit Busse bestraft werden.
Was sind geheime Personendaten?	Geheime Personendaten sind Daten, die nicht allgemein bekannt sind und bei denen die betroffene Person ein schützenswertes Interesse an der Geheimhaltung hat (z.B. Gesundheitsdaten, Daten über Einkommen oder soziale Hilfe, etc.).
Tipp	Schulen Sie Ihre Mitarbeitenden, dass Personendaten und vertrauliche Geschäftsinformationen grundsätzlich geheim gehalten werden müssen.
Tipp	Werden Ihnen Personendaten anvertraut, besprechen Sie mit der betroffenen Person, wem die Daten bekannt gegeben werden (dürfen).

IX. DIE UMSETZUNGS-CHECKLISTE

In dieser Checkliste sind die Punkte in der Reihenfolge aufgeführt, wie sie angegangen werden sollen. Nicht alles ist gleich wichtig, so dass die Prioritäten richtig gesetzt werden sollten. Die Reihenfolge kann aber auch angepasst werden. Gewisse Aufgaben können zusammen erledigt werden oder müssen fortlaufend gemacht werden.

Nr	Aufgabe	Erläuterung	OK	Verantwortung
1	**Datenschutz-person** Kapitel V	Empfehlung: Benennen Sie jemanden, der sich um den Datenschutz kümmert.	☐	
2	**Bearbeitungs-verzeichnis** Kapitel IV.A.2	Erstellen Sie ein Bearbeitungsverzeichnis. Ist kein Bearbeitungsverzeichnis notwendig, kann es dennoch sinnvoll sein, sich einen Überblick über die Datenbearbeitungen zu verschaffen und dies (vereinfacht) festzuhalten.	☐	
3	**Datenschutz-erklärung** Kapitel IV.A.1 Muster Jardin-Suisse	Erstellen Sie eine Datenschutzerklärung, die sämtliche Datenbearbeitungen enthält und halten Sie diese aktuell. Ziehen Sie dies, wenn nötig, dem Verzeichnis vor, damit sie möglichst am 01.09.2023 bereitsteht.	☐	
4	**Auftrags-bearbeiter** Kapitel IV.B.1	Prüfen Sie, ob Sie mit allen Auftragsbearbeitern und Auftragsbearbeiterinnen einen Auftragsbearbeitungsvertrag abgeschlossen haben (wo möglich zusammen mit den Auslandtransfers)	☐	
5	**Datensicherheit** Kapitel III.AIII.A	Achten Sie (fortlaufend) auf Ihre Datensicherheit. Fehlt Ihnen das Fachwissen, beauftragen Sie hierzu einen Spezialisten.	☐	
6	**Auslandtrans-fers** Kapitel IV.B.2	Prüfen Sie Ihre Auslandtransfers und Ihre diesbezüglichen Verträge.	☐	
7	**Weisung** Kapitel IV.E	Erlassen Sie eine (kurze) Weisung zum Datenschutz, welche den Umgang mit Personendaten festlegt.	☐	
8	**Schulung** Kapitel IV.E	Schulen Sie Ihre Mitarbeitenden im Umgang mit Personendaten und der Informationssicherheit.	☐	
9	**Betroffenen-rechte** Kapitel IV.C.1	Stellen Sie sicher, dass die Betroffenenrechte eingehalten werden können (z.B. Datenschutzperson)	☐	
10	**Umgang mit**	Gestalten Sie alle Datenbearbeitungen im Un-	☐	

	Personendaten Kapitel 0	ternehmen den Grundsätzen entsprechend; halten Sie sich dabei an die 10 Leitsätze.		
11	**Datenlöschung** Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**	Stellen Sie sicher, dass Personendaten gelöscht werden können und werden. Empfehlung: In einer Weisung festhalten, wie lange Daten aufbewahrt werden, sowie wann und wie sie zu löschen sind.	☐	
Tipp		Unter www.privacyscore.ch können Sie online herausfinden, wo Sie in Sachen Datenschutz stehen und erhalten konkrete Handlungsempfehlungen.		