FAQ Datenschutz Grundverordnung (DSGVO)

Was Unternehmen über das neue EU-Datenschutzrecht wissen müssen

Die in diesem FAQ enthaltenen Informationen dienen der allgemeinen Orientierung.

Sage bietet speziell zur DSGVO eine E-Mail-Adresse DSGVO@sage.de. Bitte beachten Sie, dass Sie keine rechtliche Beratung erhalten.

Rechtshinweis:

Die Inhalte wurden mit großer Sorgfalt recherchiert. Dennoch kann Sage keine Haftung für die Richtigkeit, Vollständigkeit und Aktualität der bereitgestellten Informationen übernehmen. Die Informationen sind insbesondere auch allgemeiner Art und stellen keine Rechtsberatung im Einzelfall dar. Zur Lösung von konkreten Rechtsfällen, insbesondere im Rahmen der DSGVO, konsultieren Sie bitte unbedingt einen Rechtsanwalt.

Stand: Mai 2018

Inhaltsverzeichnis

1.0	**Datenschutz**	**5**
1.1	Warum Datenschutz?	5
1.2	Ab wann gilt die DSGVO für das eigene Unternehmen?	5
1.3	Die DSGVO ist bereits am 25. Mai 2016 in Kraft getreten, wieso gilt sie dann erst zwei Jahre später?	6
1.4	Wofür gilt die DSGVO?	6
1.5	Was ist das Ziel der DSGVO?	6
1.6	Was ist der Unterschied zwischen GDPR und DSGVO?	6
1.7	Wo gilt die DSGVO?	6
1.8	Können Daten in Drittländer (= außerhalb der EU) übermittelt werden?	6
1.9	Gilt die DSGVO auch in Österreich und der Schweiz?	7
1.10	Was hat es mit den Erwägungsgründen auf sich?	7
1.11	Was sind die Unterschiede zwischen Richtlinie und Verordnung in Bezug auf die DSGVO	7
1.12	Muss die Datenschutzgrundverordnung noch in nationales Recht umgesetzt werden?	7
1.13	Wo finde ich den amtlichen Text der Datenschutzgrundverordnung?	7
1.14	Was versteht man unter den sog. "Betroffenenrechten“?	8
1.15	Was versteht man unter personenbezogenen Daten?	8
1.16	Gilt das Datenschutzrecht auch für Privatpersonen?	8
2.0	**Datenschutzbeauftragter**	**10**
2.1	Wer benötigt einen Datenschutzbeauftragten?	10
2.2	Darf jeder Datenschutzbeauftragter werden?	10
2.3	Aufgabe des Datenschutzbeauftragten	11
3.0	**Vereinbarung zur Auftragsverarbeitung**	**12**
3.1	Warum müssen neue Vereinbarungen zur Auftragsverarbeitung abgeschlossen werden?	12
3.2	Wer muss die Vereinbarung zur Auftragsverarbeitung abschließen?	12
3.3	Was gilt im Falle einer Zuwiderhandlung gegen die datenschutzrechtlichen Vorschriften der DSGVO?	12

3.4 Muss eine Vereinbarung zur Auftragsvereinbarung abgeschlossen werden, wenn momentan aktiv keine entsprechenden Produkte im Einsatz sind? 12

4.0 Mitwirkung und Meldepflichten 14
4.1 Wann muss mit den Aufsichtsbehörden zusammengearbeitet werden? 14
4.2 Müssen Datenschutzverletzungen bzw. „Datenpannen“ an die Aufsichtsbehörde gemeldet werden? 14
4.3 Muss der Betroffene der Datenschutzverletzung benachrichtigt werden? 14

5.0 Datenschutz - Folgeabschätzung 15
5.1 Wann muss ein Unternehmen eine Datenschutz-Folgeabschätzung vornehmen? 15
5.2 Wie muss die Datenschutz-Folgenabschätzung durchgeführt werden? 15
5.3 Sind die Aufsichtsbehörden auch schon vorab in die Datenschutz-Folgenabschätzung eingebunden? 15
5.4 Müssen auch die Betroffenen an der Datenschutz-Folgenabschätzung beteiligt werden? 16
5.5 Was passiert bei einem Verstoß gegen die DSGVO? 16
5.6 Wie können sich Unternehmen optimal vorbereiten? 16

6.0 Onlinehandel, Marketing 17
6.1 Können Bonitätsprüfungen durchgeführt werden? 17
6.2 Verwendung von Cookies 17
6.3 Können Social-Plugins weiterverwendet werden? 17
6.4 Was ist zu beachten, wenn Sie Einwilligungen (z.B. Newsletterversand) einholen möchten? 17
6.5 Nutzung von Kontaktformularen 18
6.6 Wie sicher ist die Kommunikation über Telefax? 18

7.0 Verarbeitungsverzeichnis 19
7.1 Muss ein Verarbeitungsverzeichnis erstellt werden? 19
7.2 Was wird aus dem Verarbeitungsverzeichnis nach dem BDSG (Bundesdatenschutzgesetz) (nur Deutschland)? 19
7.3 Was wird aus der DVR und der Meldepflicht an die zuständige Datenschutzbehörde nach dem DSG 2000? (nur Österreich) 19
7.4 Was ist Gegenstand der Meldepflicht? 20
7.5 Wann muss gemeldet werden? 20
7.6 Bei wem muss gemeldet werden? 20
7.7 Was passiert, wenn die Meldung versäumt wird? 20

7.8 Wie detailliert müssen die Angaben zum Verarbeitungsverzeichnis sein? 20

8.0 Aufbewahrungsfristen 22
8.1 Wer ist zur Aufbewahrung verpflichtet? 22
8.2 Wann beginnt und wann endet die Aufbewahrungsfrist? 22
8.3 In welcher Form müssen Unterlagen aufbewahrt werden? 22
8.4 Elektronische Rechnungen als Originale aufbewahren 23
8.5 Gibt es Dokumente, die keiner Aufbewahrungsfrist unterliegen? 23
8.6 Gibt es Dokumente die länger als 10 Jahre aufbewahrt werden müssen? 23

9.0 Checklisten 24
9.1 Checkliste zur DSGVO 24
9.2 Checkliste zum Verzeichnis der Verarbeitungstätigkeit 25
9.3 Checkliste zur Datenschutzerklärung 28

10.0 Glossar 29

1.0 Datenschutz

1.1 Warum Datenschutz?

Unter Datenschutz verstehen wir

- *Schutz vor missbräuchlicher Datenverarbeitung*
- *Schutz des Rechts auf informationelle Selbstbestimmung*
- *Schutz des Persönlichkeitsrechts bei der Verarbeitung von Daten bzw. den Schutz der Privatsphäre.*

Jeder Mensch soll grundsätzlich selbst darüber entscheiden können, wem und wann er welche seiner persönlichen Daten zugänglich macht. Der Datenschutz soll der zunehmend bestehenden Tendenz zum sog. gläsernen Menschen entgegenwirken. Kaum ein Unternehmen kann es sich noch leisten, das Thema Datenschutz und Umgang mit Kundendaten auf die leichte Schulter zu nehmen.

Hinweis: *Vielen Unternehmen ist unbekannt, dass ein betrieblicher Datenschutzbeauftragter für sie gesetzlich verpflichtend ist. Unternehmen, bei denen mehr als 9 Beschäftigte Zugriff auf personenbezogene Daten haben, benötigen einen solchen Datenschutzbeauftragten. Bei Verstößen gegen diese Pflicht drohen Bußgelder von bis zu € 25.000,00 durch die zuständige Aufsichtsbehörde.*

Die Bedeutung des Datenschutzes ist seit der Entwicklung der Digitaltechnik ständig gestiegen, weil die Weitergabe von Daten sowie deren Verarbeitung und Erfassung und Analyse immer einfacher werden. Durch das Internet wurden völlig neue Möglichkeiten zur Datenerfassung geschaffen.

Es sollte daher nicht nur jeder darauf achten, wie seine eigenen Daten verarbeitet werden, sondern auch für Unternehmen gilt die Verpflichtung, sich mit der Frage auseinanderzusetzen, welche Daten gespeichert und weiterverarbeitet werden dürfen bzw. welche Daten gelöscht werden müssen.

1.2 Ab wann gilt die DSGVO für das eigene Unternehmen?

Die DSGVO gilt ab dem 25. Mai 2018 direkt und damit für alle Unternehmen. Eine detaillierte Beschreibung zu allen Artikeln der Verordnung finden Sie unter www.dsgvo-gesetze.de

1.3 Die DSGVO ist bereits am 25. Mai 2016 in Kraft getreten, wieso gilt sie dann erst zwei Jahre später?

In Artikel 99 der DSGVO ist geregelt, dass sie ab dem 25. Mai 2018 gilt. Der frühere Zeitpunkt hat zur Folge, dass die Mitgliedsstaaten keine Regelungen mehr erlassen dürfen, die der Verordnung widersprechen und damit die Staaten die nationalen Gesetze und Änderungen auf ihre Prozesse anpassen können.

1.4 Wofür gilt die DSGVO?

Gemäß Art.2 Abs.1 DSGVO gilt die Verordnung für „die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen". Der Begriff der personenbezogenen Daten ist allerdings sehr weit gefasst und umfasst z.B. Informationen wie Name, Adresse, Telefonnummer, Autokennzeichen oder aber auch die IP-Adresse einer Person. Ausreichend ist es, wenn die Informationen einer Person irgendwie zugeordnet und damit ein Personenbezug hergestellt werden kann.

1.5 Was ist das Ziel der DSGVO?

Mit der DSGVO soll künftig ein einheitlicher Mindestschutz personenbezogener Daten innerhalb des Europäischen Binnenmarkts gewährleistet werden. Als EU-Verordnung hat die DSGVO unmittelbare Rechtswirksamkeit in allen EU-Mitgliedsstaaten. Über Öffnungsklauseln können die einzelnen Staaten jedoch bestimmte individuelle Regelungen treffen. Deutschland hat die DSGVO mit der neuen BDSG umgesetzt.

1.6 Was ist der Unterschied zwischen GDPR und DSGVO?

Die General Data Protection Regulation (GDPR) ist die englische Bezeichnung der Datenschutzgrundverordnung (DSGVO).

1.7 Wo gilt die DSGVO?

Die DSGVO stellt darauf ab, ob ein Anbieter von Waren oder Dienstleistungen personenbezogene Daten von in der EU befindlichen Personen verarbeitet, unabhängig vom Sitz des verarbeitenden Unternehmens. Die DSGVO auch dann anzuwenden, wenn die Datenverarbeitung der Beobachtung des Verhaltens von Personen in der EU dient z.B. durch die Analyse des Surfverhaltens im Internet wie auch die Speicherung von Cookies, egal zu welchem Zweck (Art. 3 Abs. 2 DSGVO).

1.8 Können Daten in Drittländer (= außerhalb der EU) übermittelt werden?

An den Grundstrukturen zur Übermittlung von personenbezogenen Daten in Drittländer ändert sich durch die DSGVO nicht viel. Wie bisher kommt es auch in Zukunft darauf an, ob im Drittland ein „angemessenes Datenschutzniveau" existiert. Sollte dies nicht der Fall sein, ist zu prüfen, ob eine Ausnahme greift, um die Datenübertragung trotz Fehlens eines angemessenen Datenschutzniveaus zu rechtfertigen (zum Beispiel Datentransfer auf

Grundlage von Standardvertragsklauseln, auf Grundlage von „Binding Corporate Rules", etc.).

1.9 Gilt die DSGVO auch in Österreich und der Schweiz?

Ja, in Österreich kommt die DSGVO ebenfalls voll zum Tragen.

Da das schweizerische Datenschutzrecht im Wesentlichen mit demjenigen der EU übereinstimmt, sind die Voraussetzungen gegeben, dass das schweizerische Recht von der EU als angemessen anerkannt wird.

Die DSGVO hat für Schweizer Unternehmen unmittelbar Geltung, da insbesondere EU Niederlassungen oder Tochtergesellschaften, in denen Daten verarbeitet werden, dem EU Datenschutz unterliegen. Gleiches gilt auch, wenn ein schweizerisches Rechenzentrum für Unternehmen in der EU tätig ist.

Das EU-Recht gilt u.a. für Schweizer Exporteure, Versandhändler, Betreiber von Plattformen für Online-Bestellungen sowie für Dienstleister, die in der EU ansässigen Personen Waren, Leistungen oder Dienstleistungen anbieten. Diese Unternehmen müssen einen Vertreter in der EU benennen, außer wenn sie Daten von in der EU ansässigen Personen nur gelegentlich bearbeiten und beinhaltet keine umfangreiche Bearbeitung von besonders schützenswerten Personendaten (z.B. Gesundheitsdaten).

1.10 Was hat es mit den Erwägungsgründen auf sich?

Die Erwägungsgründe, die in der Verordnung vor den Artikeln stehen, stellen zwar selbst keine Regelungen dar, sondern beinhalten die Motive und Gründe für die Einführung der entsprechenden Artikel. Damit helfen die Erwägungsgründe für die Auslegung der Regelungen der Artikel.

1.11 Was sind die Unterschiede zwischen Richtlinie und Verordnung in Bezug auf die DSGVO

Eine Richtlinie ist ein auf EU-Ebene verabschiedetes Dokument, das auf nationaler Ebene umgesetzt wird, jedoch mit lokalen Unterschieden. Bei einer Verordnung handelt es sich um ein auf EU-Ebene verabschiedetes Dokument, welches nicht auf nationaler Ebene umgesetzt werden muss – man spricht hier vom „One ring to rule them all", wie es bei der DSGVO der Fall ist.

1.12 Muss die Datenschutzgrundverordnung noch in nationales Recht umgesetzt werden?

Nein, die DSGVO gilt unmittelbar und direkt. Allerdings haben die nationalen Gesetzgeber noch Gestaltungspielräume, die Sie nutzen können oder zum Teil sogar nutzen müssen.

1.13 Wo finde ich den amtlichen Text der Datenschutzgrundverordnung?

Der amtliche Text der Datenschutzgrundverordnung ist im Amtsblatt der Europäischen Union vom 04. Mai 2016 veröffentlicht worden.

1.14 **Was versteht man unter den sog. "Betroffenenrechten"?**

Den betroffenen Personen (deren Daten erhoben werden) stehen umfangreiche Rechte zu, die zu beachten sind:

- *Auskunftsrecht*
- *Recht auf Vergessenwerden (Löschungsrecht)*
- *Berichtigungsrecht*
- *Recht auf Datenübertragbarkeit*
- *Widerspruchsrecht*
- *Recht auf Einschränkung der Verarbeitung*

Der Betroffene muss im Rahmen der allgemeinen Informationspflicht (= Datenschutzerklärung) auf die vorgenannten Rechte hingewiesen werden.

1.15 **Was versteht man unter personenbezogenen Daten?**

Nach der DSGVO sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Einzelangaben über persönliche oder sachliche Verhältnisse sind beispielsweise:

- *Name, Alter, Familienstand, Geburtsdatum,*
- *Anschrift, Telefonnummer, E-Mail Adresse*
- *Konto-, Kreditkartennummer*
- *Kraftfahrzeugnummer, Kfz-Kennzeichen*
- *Personalausweisnummer, Sozialversicherungsnummer*
- *Vorstrafen*
- *genetische Daten und Krankendaten*
- *Werturteile wie zum Beispiel Zeugnisse*

Kundendaten gehören ebenso zu den personenbezogenen Daten wie die Personaldaten von Beschäftigten. Auch Fotos, Videoaufnahmen, Röntgenbilder oder Tonbandaufnahmen können personenbezogene Daten enthalten.

1.16 **Gilt das Datenschutzrecht auch für Privatpersonen?**

Grundsätzlich müssen auch Privatpersonen, die personenbezogene Daten erheben, verarbeiten oder nutzen die DSGVO beachten. Dies gilt allerdings nicht, wenn die Datenverarbeitung ausschließlich für persönliche oder familiäre Zwecke erfolgt. Erstellen Sie beispielsweise elektronische Adressbücher oder Geburtstagslisten, um diese für

persönliche Zwecke zu nutzen, ist dies in der Regel unproblematisch. Stellen sie hingegen Informationen über andere Personen in das Internet, machen Sie damit diese Daten Dritten zugänglich. So handelt es sich beispielsweise nicht mehr um eine Verarbeitung ausschließlich zu persönlichen Zwecken, wenn durch Zustimmung an Whatsapp, Xing oder LinkedIn auf ihr persönliches Adressbuch zugegriffen wird.

2.0 Datenschutzbeauftragter

2.1 Wer benötigt einen Datenschutzbeauftragten?

Für Deutschland:

Der Datenschutzbeauftragte muss gemäß § 4 f Bundesdatenschutzgesetz (BDSG) bei öffentlichen und nicht-öffentlichen Stellen, die personenbezogene Daten automatisiert verarbeiten, schriftlich bestellt werden, wenn mehr als 9 Mitarbeiter ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Unter automatisierter Verarbeitung versteht man die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten in der EDV. Ebenso wird ein Datenschutzbeauftragter benötigt, wenn mehr als 19 Personen nicht - automatisierte personenbezogene Daten verarbeiten.

Für Österreich:

Eine Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht für Unternehmen (Verantwortliche und Auftragsverarbeiter), wenn

- *die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfanges und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen, oder*

- *die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten oder von Daten über strafrechtliche Verurteilungen oder Straftaten besteht*

Hinweis: *Auch ohne Datenpanne drohen empfindliche Bußgelder und Auflagen, negative Presse inklusive (z. B. bei Nichtbestellung eines Datenschutzbeauftragten).*

2.2 Darf jeder Datenschutzbeauftragter werden?

Sofern er über die erforderliche Sachkunde und Unabhängigkeit verfügt, im Prinzip ja. So kann es Geschäftsführern und Leitenden Angestellten an der notwendigen Unabhängigkeit fehlen. Zudem ist es wünschenswert, sich möglichst gut mit IT-Systemen, Organisation und den gesetzlichen Grundlagen des Datenschutzes auszukennen.

2.3 **Aufgabe des Datenschutzbeauftragten**

Der betriebliche Datenschutzbeauftragte hat auf die Einhaltung datenschutzrechtlicher Bestimmungen im Unternehmen hinzuwirken. Gleichzeitig ist er Ansprechpartner für Kunden, Mitarbeiter, Geschäftsleitung und Betriebsrat bei Datenschutzfragen.

Er hat insbesondere:

- *die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,*

- *die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.*

Schwerpunkte der Tätigkeit eines betrieblichen Datenschutzbeauftragten sind z. B.:

- *Telekommunikationsdatenschutz*
- *Gesundheitsdatenschutz*
- *Auftragsdatenverarbeitung*
- *Cloud Computing und Datenschutz*

3.0 Vereinbarung zur Auftragsverarbeitung

3.1 Warum müssen neue Vereinbarungen zur Auftragsverarbeitung abgeschlossen werden?

Die DSGVO verfolgt das Ziel einer EU-weiten Harmonisierung der Zusammenarbeit bei der Verarbeitung personenbezogener Daten. Durch stärkere und präzisere Rechte für betroffene Personen und verschärfte Verpflichtungen für Verarbeiter von Daten, soll ein EU-weiter wirksamer Schutz personenbezogener Daten möglich werden. Dies bedingt auch eine Änderung der Vereinbarung zur Auftragsverarbeitung.

3.2 Wer muss die Vereinbarung zur Auftragsverarbeitung abschließen?

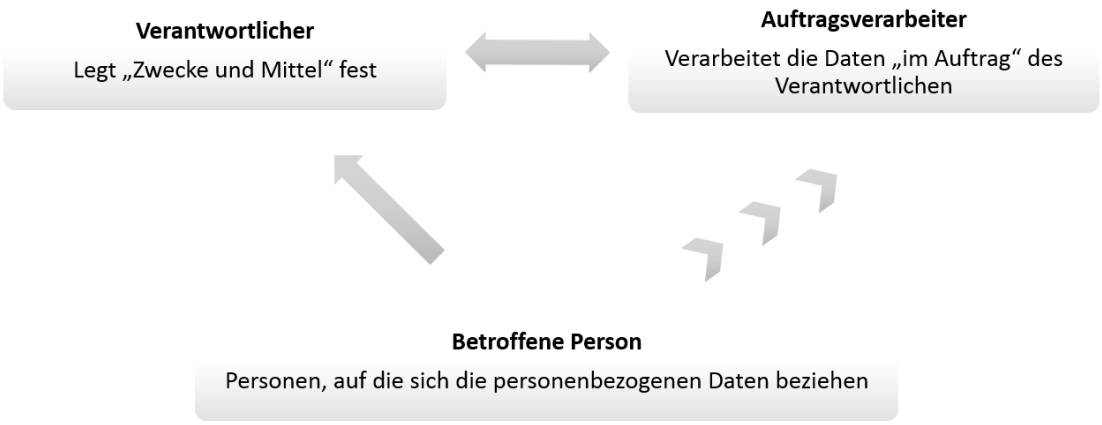
Jeder Kunde mit direkter Vertragsbeziehung - unabhängig davon, welche Produkte er nutzt muss eine Vereinbarung abschließen.

3.3 Was gilt im Falle einer Zuwiderhandlung gegen die datenschutzrechtlichen Vorschriften der DSGVO?

Verstoßen z.B. Online-Händler gegen die Vorgaben zur Auftragsverarbeitung, drohen Bußgelder bis zu 10 Millionen Euro oder von bis zu 2 % des gesamten weltweiten Jahresumsatzes - je nachdem, welcher Betrag der höhere ist. Bei schweren Verstößen gegen die Pflichten des Verantwortlichen sollen Geldbußen bis zu 20 Millionen Euro oder von bis zu 4% des gesamten weltweit erzielten unternehmerischen Jahresumsatzes verhängt werden können. Zudem drohen auch wettbewerbsrechtliche Abmahnungen.

3.4 Muss eine Vereinbarung zur Auftragsvereinbarung abgeschlossen werden, wenn momentan aktiv keine entsprechenden Produkte im Einsatz sind?

Bitte schließen Sie in jedem Fall eine Vereinbarung zur Auftragsvereinbarung ab, da ab dem 25.05.2018 eine Vereinbarung zur Auftragsverarbeitung zwingend notwendig ist, sobald Sie dem Auftraggeber personenbezogene Daten zur Verarbeitung überlassen.


Verantwortlicher
Legt „Zwecke und Mittel“ fest
Auftragsverarbeiter
Verarbeitet die Daten „im Auftrag“ des Verantwortlichen
Betroffene Person
Personen, auf die sich die personenbezogenen Daten beziehen

4.0 Mitwirkung und Meldepflichten

4.1 Wann muss mit den Aufsichtsbehörden zusammengearbeitet werden?

Immer dann, wenn es die Aufsichtsbehörde zur Erfüllung ihrer Aufgaben verlangt.

4.2 Müssen Datenschutzverletzungen bzw. „Datenpannen" an die Aufsichtsbehörde gemeldet werden?

Ja. Der Verantwortliche muss ohne schuldhaftes Zögern und möglichst binnen 72 Stunden nachdem die Datenverletzung bekannt wurde, dies der zuständigen Aufsichtsbehörde melden. Der Auftragsdatenverarbeiter muss daher ebenfalls eine „Datenpanne" unverzüglich an den Auftraggeber melden, damit dieser wiederum seiner Meldepflicht nachkommen kann.

Kann ein Risiko für Rechte und Freiheiten von Individuen ausgeschlossen werden oder als höchst unwahrscheinlich eingestuft werden, entsteht keine Meldepflicht.

4.3 Muss der Betroffene der Datenschutzverletzung benachrichtigt werden?

Ja. Die Benachrichtigung sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene Person gerichtete Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen dieser Verletzung enthalten. Eine Benachrichtigung sollte somit so rasch, wie nach allgemeinen Ermessen möglich, erfolgen.

Wenn technische oder organisatorische Maßnahmen wie z. B. eine Verschlüsselung die Kenntnisnahme von personenbezogenen Daten verhindern oder sicherstellen, dass kein hohes Risiko besteht, muss der Betroffene allerdings nicht benachrichtigt werden.

5.0 Datenschutz - Folgeabschätzung

Gänzlich neu eingeführt wird die Pflicht zur Datenschutz-Folgeabschätzung.

5.1 Wann muss ein Unternehmen eine Datenschutz-Folgeabschätzung vornehmen?

Sie ist immer dann durchzuführen, wenn ein Datenverarbeitungsverfahren voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen birgt. Dies ist insbesondere der Fall bei der Verwendung neuer Technologien oder sonst aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung. Für Auftragsverarbeiter ist das insofern relevant, als diese stärker als zuvor verpflichtet werden, den Auftraggeber hierbei zu unterstützen.

Ist in dem Unternehmen ein Datenschutzbeauftragter bestellt, muss er in die Datenschutz-Folgenabschätzung eingebunden werden. Die Datenschutz-Folgenabschätzung ist schriftlich zu dokumentieren.

5.2 Wie muss die Datenschutz-Folgenabschätzung durchgeführt werden?

Die Folgenschutzabschätzung erfolgt in 3 Stufen:

- *In der 1. Stufe ist zu prüfen, ob ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht. Hauptanwendungsgebiete sind bei Technologien, die automatisiert, systematisch und umfassend Daten erfassen, verarbeiten und bewerten, gegeben.*
- *Besteht ein solches Risiko, ist in einer 2. Stufe eine Bewertung vorzunehmen, ob die geplanten Abhilfemaßnahmen und Sicherheitsvorkehrungen ausreichen, um den Schutz der Daten zu gewährleisten. Zudem muss der Nachweis erbracht werden, dass die DSGVO eingehalten und den Interessen der Betroffenen Rechnung getragen wird.*
- *Kommt die Bewertung zu dem Ergebnis, dass trotz möglicher Maßnahmen ein hohes Risiko besteht, muss in einer 3. Stufe die Aufsichtsbehörde konsultiert werden. Diese spricht dann innerhalb von 8 Wochen eine schriftliche Empfehlung zur Risikominimierung aus; sie darf die Datenverarbeitung aber auch vollständig untersagen. Je nach Komplexität kann die Frist von der Aufsichtsbehörde auch verlängert werden.*

5.3 Sind die Aufsichtsbehörden auch schon vorab in die Datenschutz-Folgenabschätzung eingebunden?

Da die Aufsichtsbehörden unabhängig vom Risiko für besonders sensible Fälle die zwingende Durchführung der Folgenabschätzung anordnen können, ist sie bereits im Vorfeld mit einzubinden. Die Aufsichtsbehörden werden Technologien nach ihrem

Datenschutzrisiko klassifizieren und entsprechende Positiv-/Negativ-Listen veröffentlichen.

5.4 Müssen auch die Betroffenen an der Datenschutz-Folgenabschätzung beteiligt werden?

Ja und zwar dann, wenn es als angemessen erscheint.

5.5 Was passiert bei einem Verstoß gegen die DSGVO?

Durch die DSGVO wird die Haftung erheblich verschärft. Eine natürliche Person, die einen Schaden durch einen Verstoß gegen die DSGVO erleidet, hat Anspruch auf Schadensersatz – sowohl bei materiellen als auch bei immateriellen Schäden. Schadensersatzpflichtig ist der Verantwortliche und jeder an der Verarbeitung Beteiligte, damit auch ein Auftragsverarbeiter.

Neben den aufsichtsbehördlichen Maßnahmen steigt zudem die Gefahr von Abmahnungen.

Achtung: *Es drohen bei Verstößen gegen die DSGVO empfindliche Geldbußen für die Unternehmen. So können Bußgelder bis zu 20 Millionen Euro oder bis zu 4% des weltweiten Umsatzes des letzten Geschäftsjahres verhängt werden.*

5.6 Wie können sich Unternehmen optimal vorbereiten?

Um sich optimal auf die Regelungen der DSGVO vorzubereiten, sollten Unternehmen sich vor allem klarmachen: es wird Ernst und die Zeit läuft.

Geschäftsführer, Datenschutzbeauftragte und andere für den Datenschutz in einem Unternehmen Verantwortliche müssen sich dafür sensibilisieren, dass ab dem 25. Mai 2018 nicht nur der Name der Datenschutzvorschrift geändert wird. Die DSGVO wird in vielen Bereichen direkte Auswirkung auf jedes datenverarbeitende Unternehmen haben.

Konflikte mit Nutzern, Abmahnungen und Bußgelder kann es auch wegen verspäteter Anpassung an die DSGVO geben, die sich jedoch vermeiden lassen, wenn Sie unverzüglich mit einer sorgfältigen Maßnahmenplanung und – umsetzung beginnen. Sage unterstützt Sie gerne. Erfahren Sie mehr zu unseren Angeboten der Sage Academy.

6.0 Onlinehandel, Marketing

6.1 Können Bonitätsprüfungen durchgeführt werden?

Ja, wenn die Entscheidung über den Abschluss eines Vertrags von der Bonitätsprüfung abhängt (wie z.B. beim Rechnungskauf im Online-Shop), kann eine Bonitätsprüfung wie bisher durchgeführt werden. Notwendig ist die Aufnahme einer Interessenabwägung im Rahmen der Datenschutzerklärung.

6.2 Verwendung von Cookies

Wie bisher werden Cookies als personenbezogene Daten behandelt. Daher wird eine Rechtfertigung für den Einsatz von Cookies benötigt. Für den Einsatz von Cookies ist ein „berechtigtes Interesse" notwendig.

Erforderlich ist eine sorgfältig durchgeführte Interessenabwägung für die Beurteilung eines berechtigten Interesses.

In Ausnahmefällen ist die Einholung einer Einwilligung notwendig, aber auch hier gilt: Die Datenschutzerklärung sollte so konzipiert sein, dass genau mitgeteilt wird, wie die Einwilligung eingeholt werden muss.

6.3 Können Social-Plugins weiterverwendet werden?

Die Social Plugins werden durch die DSGVO zwar nicht beendet, doch da das Datenschutzrecht in den Fokus der Datenschützer rückt, sollten insbesondere Shop-Betreiber entweder ganz auf Plugins verzichten oder auf datenschutzkonforme Lösungen zurückgreifen.

6.4 Was ist zu beachten, wenn Sie Einwilligungen (z.B. Newsletterversand) einholen möchten?

Einwilligungen nach der DSGVO unterliegen strengen Vorgaben. Folgende Voraussetzungen müssen nach der DSGVO erfüllt werden:

- *Informiertheit: Es muss z.B. in Zusammenhang mit Einwilligungen über die Identität des Datenverarbeiters (in der Regel Online-Händler), über die Zwecke der Datenverarbeitung und ein jederzeitiges, freies Widerrufsrecht informieren werden.*
- *Beachtung des Kopplungsverbots: Unter Umständen können vertragliche Einigungsklauseln unwirksam sein, wenn sich diese auf Daten erstrecken, die für die Erfüllung des Vertrages nicht erforderlich sind.*

- *„Klares Ungleichgewicht": Einwilligungserklärungen sind unwirksam, wenn ein sogenanntes „klares Ungleichgewicht" zwischen dem Verantwortlichen und dem Betroffenen gegeben ist.*
- *Widerrufsmöglichkeit: Einwilligungserklärungen sind jederzeit mit Wirkung für die Zukunft frei widerruflich.*
- *Form: Die Einwilligung kann durch eindeutige, bestätigende Handlung in Form einer schriftlichen, elektronischen oder mündlichen Erklärung erfolgen (es genügt hierzu auch ein Mausklick).*
- *Minderjährige: Minderjährige unter 16 Jahren können keine wirksamen Einwilligungserklärungen abgeben (es kommt dann auf die Einwilligung der Erziehungsberechtigten an).*

6.5 Nutzung von Kontaktformularen

Diese können weiterhin verwendet werden. Nehmen Sie hierzu einen entsprechenden Hinweis in Ihrer Datenschutzerklärung vor.

Beachte Sie, dass Kontaktformulare verschlüsselt werden müssen, um den Vorgaben aus dem Grundsatz der Integrität und Vertraulichkeit gerecht zu werden.

6.6 Wie sicher ist die Kommunikation über Telefax?

Beim Telefaxverfahren handelt es sich um einen Dienst, der grundsätzlich keine Datensicherheitsmaßnahmen enthält, der das Telefonnetz als Transportweg nutzt und in der Regel einen offenen Ausdruck beim Empfang entstehen lässt. Die Sorglosigkeit im Umgang mit diesem Medium groß. Fehlerhaft adressierte oder fehlgeleitete Faxe bleiben zwar häufig folgenlos, doch können sie in einzelnen Fällen eine erhebliche Beeinträchtigung für die Betroffenen nach sich ziehen.

Wichtig: *Das Versenden vertraulicher Informationen via Telefax ist nach DSGVO Gesichtspunkt riskant und sollte insbesondere beim Versand von sensiblen, personenbezogenen Unterlagen im Regelfall nicht via Fax erfolgen.*

7.0 Verarbeitungsverzeichnis

Die DSGVO sieht neue Dokumentationsanforderungen vor, die über die bisherigen Anforderungen nach dem deutschen/österreichischen Recht hinausgehen.

7.1 Muss ein Verarbeitungsverzeichnis erstellt werden?

Ab Mai 2018 muss ein schriftliches oder elektronisches Verzeichnis über alle Verarbeitungstätigkeiten mit personenbezogenen Daten erstellt werden. Die Verantwortlichen und die Auftragsverarbeiter sind dazu verpflichtet, dieses auf Anfrage der Datenschutzaufsichtsbehörde zur Verfügung zu stellen.

7.2 Was wird aus dem Verarbeitungsverzeichnis nach dem BDSG (Bundesdatenschutzgesetz) (nur Deutschland)?

Die Führung des Melderegisters wird zum 25. Mai 2018 eingestellt, d. h. die bisher in § 4d und § 4e BDSG geregelte Meldepflicht von einigen verantwortlichen Stellen wird entfallen. Das öffentlich von jedermann einsehbares Verzeichnis bei der Aufsichtsbehörde wird nicht mehr fortgeführt.

Die unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) haben neue Mustervorlagen sowie ausführliche Hinweise zum Verzeichnis von Verarbeitungstätigkeiten abgestimmt und veröffentlicht.

Achtung: *Wenn die Meldung versäumt wird, kann ein Bußgeld erhoben werden. Datenverarbeitende Stellen, die der Meldepflicht nicht unterliegen, erstellen über ihre Verfahren zur Verarbeitung personenbezogener Daten ein eigenes Verarbeitungsverzeichnis.*

7.3 Was wird aus der DVR und der Meldepflicht an die zuständige Datenschutzbehörde nach dem DSG 2000? (nur Österreich)

Mit dem In-Geltung-Treten der EU-Datenschutz-Grundverordnung am 25. Mai 2018 entfällt die Verpflichtung zur Erstattung von DVR-Meldungen an die Datenschutzbehörde. Das Datenverarbeitungsregister wird ab diesem Zeitpunkt (bis zum 31. Dezember 2019) zu Archivzwecken fortgeführt werden und kann mithilfe der Exportfunktion im DVR-Online gesichert werden.

Weiterführenden Informationen dazu finden Sie auf der Seite der Datenschutzbehörde. (https://www.dsb.gv.at/datenschutz-grundverordnung)

7.4 **Was ist Gegenstand der Meldepflicht?**

Grundsätzlich müssen alle Verfahren automatisierter Verarbeitungen personenbezogener Daten bei der Datenschutzaufsichtsbehörde gemeldet werden. Unter Verfahren ist die Gesamtheit an Verarbeitungen zu verstehen, mit denen eine oder mehrere miteinander verbundene Zweckbestimmung(en) realisiert werden sollen. Daher kann ein Verfahren eine Vielzahl von Datenverarbeitungsdateien umfassen.

Die Verfahren automatisierter Verarbeitungen, in denen personenbezogene Daten geschäftsmäßig

- *zum Zweck der Übermittlung (z. B. Auskunftstätigkeit, Adresshandel)*
- *zum Zweck der anonymisierten Übermittlung (z. B. Markt- und Meinungsforschung)*

gespeichert werden, sind ohne Ausnahme meldepflichtig.

7.5 **Wann muss gemeldet werden?**

Die Meldung hat bereits vor der Inbetriebnahme des meldepflichtigen Verfahrens zu erfolgen. Auch Änderungen der meldepflichtigen Angaben und die Beendigung des meldepflichtigen Verfahrens sind jeweils im Voraus mitzuteilen.

7.6 **Bei wem muss gemeldet werden?**

Die Meldung muss bei der zuständigen Aufsichtsbehörde für den Datenschutz erfolgen, in deren Aufsichtsbezirk die meldepflichtige Stelle ihren Sitz hat. An welchem Ort im Inland die Datenverarbeitung erfolgt, ist für die Meldung also unerheblich. Wenn die meldepflichtige Stelle ihren Sitz außerhalb der Europäischen Union und außerhalb eines Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum (EWR: Island, Norwegen und Liechtenstein) hat, muss die Meldung bei der Aufsichtsbehörde erfolgen, in deren Zuständigkeitsbereich der im Inland ansässige Vertreter der meldepflichtigen Stelle seinen Sitz hat.

7.7 **Was passiert, wenn die Meldung versäumt wird?**

Wenn eine verantwortliche nicht-öffentliche Stelle vorsätzlich oder fahrlässig eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vornimmt, begeht eine Ordnungswidrigkeit, die mit einer Geldbuße bis zu 50.000 Euro geahndet werden kann.

7.8 **Wie detailliert müssen die Angaben zum Verarbeitungsverzeichnis sein?**

- *Zweckbestimmungen der Datenerhebung, -verarbeitung oder –nutzung:*

  Es müssen gesonderte Angaben zu jedem Verfahren vorgenommen werden, aus denen ersichtlich ist, welche Zwecke/Ziele konkret verfolgt werden. Formelhafte Angaben, wie zum Beispiel „alle banküblichen Geschäfte", sind unzureichend.

- *Beschreibung der betroffenen Personengruppen und der Daten/Datenkategorie:*

  Mit Daten sind „Datenfeldbezeichnungen" gemeint. Werden Datenkategorien angegeben, so müssen diese so konkret wie möglich sein. Die Beschreibung der Daten/Datenkategorien soll stets verdeutlichen, was in Bezug auf die Betroffenen gespeichert wird. Wesentlich ist eine detaillierte Darstellung der Datenkategorien. Beispiel:

  Kundendaten - nicht ausreichend = zu allgemein
  Anschriften - ausreichend = Datenkategorie
  Straße, Haus Nr., PLZ, Stadt usw. - ausreichend = Daten (Datenfelder).
  Corneliusstr., 27, 40217, Düsseldorf usw. - unzulässig = personenbezogene Daten

- *Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können:*

  Es kann hier entweder der konkrete Empfänger, an die Daten übermittelt werden, oder lediglich Empfängerkategorien angeben werden. Für Datenkategorien gilt, dass eine abstrahierende Zusammenfassung von bestimmten Empfängergruppen möglich ist. Die Bezeichnung muss hinreichend konkret und für Außenstehende verständlich sein. Eine allgemeine Bezeichnung wie „Kunden" genügt nicht. Mindestens muss erkennbar sein, in welcher Branche oder welchem Betätigungsfeld die Kunden aktiv sind. So könnte eine Empfängerkategorie beispielsweise „Telekommunikationsunternehmen" oder „Versandhandelsunternehmen" lauten.

- *Regelfristen für die Löschung der Daten:*

  Es genügt nicht, sich auf die „gesetzlichen Aufbewahrungsfristen" zu berufen. Um die geforderte Transparenz zu ermöglichen, müssen möglichst konkrete Angaben gemacht werden. Unter Umständen reicht die Nennung der einschlägigen Vorschriften aus, wenn eine konkretere Antwort nicht möglich ist.

- *Datenübermittlung in Drittstaaten:*

  Die Angabe der Datenübermittlungen in Drittstaaten (Drittstaaten sind alle Staaten, die weder der EU noch dem EWR angehören) sind bereits dann zu tätigen, wenn es mit einer gewissen Wahrscheinlichkeit zu einer Übermittlung kommen wird. Zeitpunkt und nähere Umstände brauchen nicht festzustehen. Bei der Erstanmeldung zum Register sind bereits bestehende Übermittlungen zu melden. Hingegen brauchen bei Änderungsmitteilungen wegen neu geplanter Übermittlungen in Drittstaaten bereits bestehende (und gemeldete) Übermittlungen nicht erneut gemeldet zu werden.

  Eine dahingehende Pauschalisierung, dass die Datenlieferung „in alle Länder der Welt" möglich sei, ist nicht zulässig. Der Gesetzgeber hat die „Drittstaaten"-Meldepflicht eingeführt, um die Zulässigkeit einer Übermittlung im Einzelfall anhand der datenschutzrechtlichen Bestimmungen des Empfängerlandes beurteilen zu können. Für den Bereich der EU und des EWR geht der Gesetzgeber von einem gleichwertigen Datenschutzniveau aus und verzichtet auf die Meldung. Es sind konkret die Länder anzugeben, in die Übermittlungen stattfinden oder geplant sind.

8.0 Aufbewahrungsfristen

8.1 Wer ist zur Aufbewahrung verpflichtet?

Die Aufbewahrungspflicht ist Teil der steuerlichen und handelsrechtlichen Buchführungs- und Aufzeichnungspflicht. Generell ist somit jeder Gewerbetreibende, der nach Steuer- oder Handelsrecht zum Führen von Büchern und Aufzeichnungen verpflichtet ist, diese auch für eine bestimmte Zeit aufzubewahren. Je nach Dokumententyp müssen die Dokumente entweder 6 Jahre oder 10 Jahre archiviert werden. Eine detaillierte Auflistung zu den Aufbewahrungsfristen finden Sie im Dokument „Aufbewahrungsfristen".

Hinweis: *Auch Privatleute haben eine Aufbewahrungspflicht zu beachten. Sie bezieht sich auf Rechnungen, Zahlungsbelege oder andere beweiskräftige Unterlagen, die Privatpersonen im Zusammenhang mit Leistungen erhalten haben. Zu solchen Leistungen gehören u. a. sämtliche Bauleistungen, planerische Leistungen, die Bauüberwachung, Renovierungsarbeiten, das Anlegen von Bepflanzungen oder der Gerüstbau. Auf diese Aufbewahrungspflicht hat der leistende Unternehmer nach dem UStG in der Rechnung hinzuweisen.*

8.2 Wann beginnt und wann endet die Aufbewahrungsfrist?

Maßgebend für die Berechnung der Aufbewahrungsfrist ist lediglich das Jahr, nicht das genaue Datum des Dokuments. Ein Dokument, das am 31. Dezember 2007 erstellt wurde, hat seine 10 Jahre Aufbewahrungsfrist zum 1. Januar 2018 ebenso erreicht, wie ein Dokument mit dem Erstellungsdatum 2. Januar 2007. Letzteres muss also streng genommen sogar 11 Jahre lang aufbewahrt werden.

Länger aufbewahrt werden müssen Buchhaltungsbelege auch, wenn der Abschluss nicht im gleichen Jahr, sondern erst später erfolgt. Wurden beispielsweise Belege aus 2007 erst 2008 gebucht oder der Abschluss für das Jahr 2007 erst 2008 fertiggestellt, beginnt die 10jährige Aufbewahrungsfrist für die Belege erst mit Ablauf des Jahres 2008. Solche Belege dürfen erst am 1. Januar 2019 entsorgt werden, nicht schon 2018.

8.3 In welcher Form müssen Unterlagen aufbewahrt werden?

Unterlagen, die steuerrechtlich relevant und zugleich im Original digital erstellt wurden, müssen in einer Form aufbewahrt werden, die eine maschinelle Auswertung ermöglicht. Bedeutet, dass für solche Unterlagen die bildliche Wiedergabe auf Papier, Mikrofilm oder als Image nicht ausreicht. Bedingt durch die GoBD Richtlinie aus Jahr 2014, wurden in diesem Zusammenhang weitreichende Änderungen vorgenommen, so dass Papier-Archive den digitalen Archiven gleichgesetzt wurden.

8.4 Elektronische Rechnungen als Originale aufbewahren

Elektronische Rechnungen sind in der Form aufzubewahren, in der sie eingegangen/ erstellt worden sind. Unzulässig ist ein sog. „Medienbruch", also die Umwandlung des Dokuments, z.B. durch Ausdruck einer elektronischen Rechnung. Konvertierungen sind lediglich insoweit zulässig, als ein intern automatisch weiterverarbeitbares Format gewählt wird. Bei einer Konvertierung muss das Original trotzdem aufbewahrt werden.

Wichtig: *Der Datenträger, auf dem das Dokument aufbewahrt wird, darf keine nachträgliche Veränderung zulassen.*

8.5 Gibt es Dokumente, die keiner Aufbewahrungsfrist unterliegen?

Ja, es gibt Dokumente die sofort entsorgt werden dürfen. Dazu gehören beispielsweise Angebote, die nicht zu einem Auftrag führten oder Halbjahresbilanzen. Jahresbilanzen dagegen müssen 10 Jahren archiviert werden.

8.6 Gibt es Dokumente die länger als 10 Jahre aufbewahrt werden müssen?

In bestimmten Fällen müssen Dokumente aufbewahrt werden, obwohl sie ihr gesetzliches „Verfallsdatum" bereits überschritten haben. Dies ist beispielsweise dann der Fall, wenn sie zu einem schwebenden Verfahren gehören:

- *eine laufende Betriebsprüfung, die sich auf den verjährten Zeitraum bezieht*
- *eine bußgeldrechtliche oder eine Steuer-Strafermittlung*
- *ein schwebendes Rechtsbehelfsverfahren*
- *eine vorläufige Steuerfestsetzung*

Achtung: *Beachten Sie, dass es sich bei dieser Aufzählung lediglich um Beispiele und keine vollständige Aufzählung handelt. Bitte sprechen Sie vor der Vernichtung Ihrer Unterlagen in jedem Fall mit Ihrem Rechtsbeistand bzw. Steuerberater.*

Weitere Information zu den unterschiedlichen Aufbewahrungsfristen finden Sie unter „Übersicht der Aufbewahrungsfristen".

9.0 Checklisten

9.1 Checkliste zur DSGVO

Projektplan erstellen, *um die einzelnen Anforderungen umzusetzen.*

Auftragsverarbeitung
Mit Dienstleistern, die personenbezogene Daten für Ihr Unternehmen im Auftrag verarbeiten, muss ein Vertrag zur Auftragsverarbeitung geschlossen werden.

Vertragsmanagement
Haftungs- und Datenschutzregeln in Verträgen prüfen, Betriebsvereinbarungen überarbeiten - es ist auf die Rechte der betroffenen Beschäftigten einzugehen, z. B. auf Auskunfts- und Löschungsrechte.

Formulare und Einwilligungen ändern
Bei jeder Einwilligung muss über die Widerrufsmöglichkeiten informiert werden. Bei Einwilligungserklärungen zu besonderen personenbezogenen Daten wie Gesundheitsdaten sind Verbote zu prüfen, die der Einwilligung entgegenstehen. Demgegenüber ist für Einwilligungen keine Schriftform mehr erforderlich.

Datenübermittlungen
in Drittstaaten überprüfen z. B. in Bezug auf EU-Standardvertragsklauseln

Datenschutzbeauftragten bestellen und einsetzen
Ein in- oder externer Datenschutzbeauftragter muss bestellt werden, wenn mehr als 9 Mitarbeiter ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Er hat die Funktion eines Kontrollorgans inne und ist zusammen mit der Geschäftsleitung u. a. für interne Datenschutzschulungen zuständig. (nur DE, für AT siehe Kapitel 2.0)

Datenschutzerklärungen und Webtracking anpassen
ebenso müssen Kundenmaterialien, in denen Bezug auf die Verarbeitung personenbezogener Daten genommen wird, angepasst werden. Beim Webtracking, z. B. mittels Google Analytics, oder das Schalten von

personalisierter Werbung mittels Cookies sollten geplante Werbemaßnahmen im Online-Marketing frühzeitig auf den Prüfstand gestellt werden.

Neue Prozesse einrichten/Prozesshandbuch erstellen
Mit der DSGVO entstehen verschiedene Pflichten, für die entsprechende Prozesse eingeführt werden müssen. Insbesondere für die Dokumentations-pflicht sollten Ressourcen geschaffen werden:

- *Betroffenenrechte (z. B. Informationsanfragen von Kunden, die über die Verarbeitung ihrer Daten informiert werden möchten)*
- *Vorgehensweise zu Kundenanfragen beschreiben, die erfahren möchten, welche Daten von ihnen gespeichert wurden?*
- *Die Vorgehensweise bei erklärten Widersprüchen von Kunden muss ebenfalls in einer Prozessbeschreibung festgehalten werden*
- *Prozessbeschreibung, wenn ein Kunde darauf besteht, dass seine Daten gelöscht werden. Verantwortlichkeiten klären.*
- *Meldepflichten bei Datenpannen, wenn es z.B. zu einem Datenleck kommt und personenbezogene Daten in falsche Hände geraten.*

  Achtung: *Kommen Daten abhanden, zum Beispiel durch einen Hackerangriff, müssen Unternehmen binnen 72 Stunden die zuständige Landesdatenschutzbehörde informieren!*

- *Ist das Ziel, warum Daten gespeichert wurden, erreicht, müssen die Daten gelöscht werden (Bei einem Gewinnspiel etwa nach der Ermittlung der Gewinner). Es muss beschrieben werden, wie der Löschprozess organisiert ist.*
- *Schulung der Mitarbeiter, damit sie die Prozesse kennen und ausführen (durch den Datenschutzbeauftragten)*
- *Anlage der Datenschutz-Folgenabschätzung*
- *Erstellung eines Verarbeitungsverzeichnisses*

9.2 Checkliste zum Verzeichnis der Verarbeitungstätigkeit

Jedes Unternehmen muss ein sogenanntes „Verzeichnis der Verarbeitungstätigkeiten" anlegen. Dies kann beispielsweise in einer Tabelle erfolgen. Wir wollen Ihnen im Folgenden zwei Beispiele aufzeigen, wie Sie dies gestalten können.

Abgefragt werden sollte:

- *Welche Informationen erhalten Betroffene (zum Beispiel die Kunden) über die Erhebung und Speicherung personenbezogener Daten?*

- *Wie werden diese Informationen erteilt: Stehen Sie zum Beispiel in den AGB, in einem Text neben einer Checkbox auf der Website oder teilt man sie mündlich mit?*

- *Welche Daten werden erhoben, welchem Zweck dient die Datenerhebung, wie werden diese Daten weiterverarbeitet? Daraus leitet sich ab, ob es eine gesetzliche Erlaubnis gibt, die Daten zu verarbeiten – etwa bei einer Vertragsbeziehung – oder ob der Betroffene der Datenverarbeitung erst zustimmen muss.*

- *Werden Daten anonymisiert oder pseudonymisiert?*

- *Wie lange werden die Daten gespeichert?*

- *Werden die Daten weitergegeben? Wenn ja, an wen? Ist dieser ebenfalls für den Datenschutz verantwortlich?*

- *Wo werden die Daten gespeichert? Werden sie außerhalb der EU gespeichert? Falls ja: Sind die Voraussetzungen zur Übermittlung in Drittstaaten erfüllt?*

- *Werden die Daten ausreichend durch technische und organisatorische Maßnahmen geschützt?*

1. Kundenstammdaten

Verantwortlich	*Geschäftsführer Franz Arber, Adresse, Telefonnummer*
Zweck	*Termin- und Auftragsentgegennahme, Erbringung von Dienstleistungen*
Betroffene	*Kunden des Großhandels Arber*
Wer kann auf die Daten zugreifen?	*Alle Mitarbeiter des Großhandels Arber*
Datenkategorie	*Kundenstammdaten (Name, Telefonnummer, E-Mail-Adresse)* *Großhandel (Elektroklein- und großgeräte, Dienstleistungen, bevorzugter Elektriker)*
Übermittlung an Drittstaaten	*Nein*
Löschfrist	*Bei Widerruf des Betroffenen*
Rechtsgrundlage	*DSGVO Art. 6, Abs. 1b*

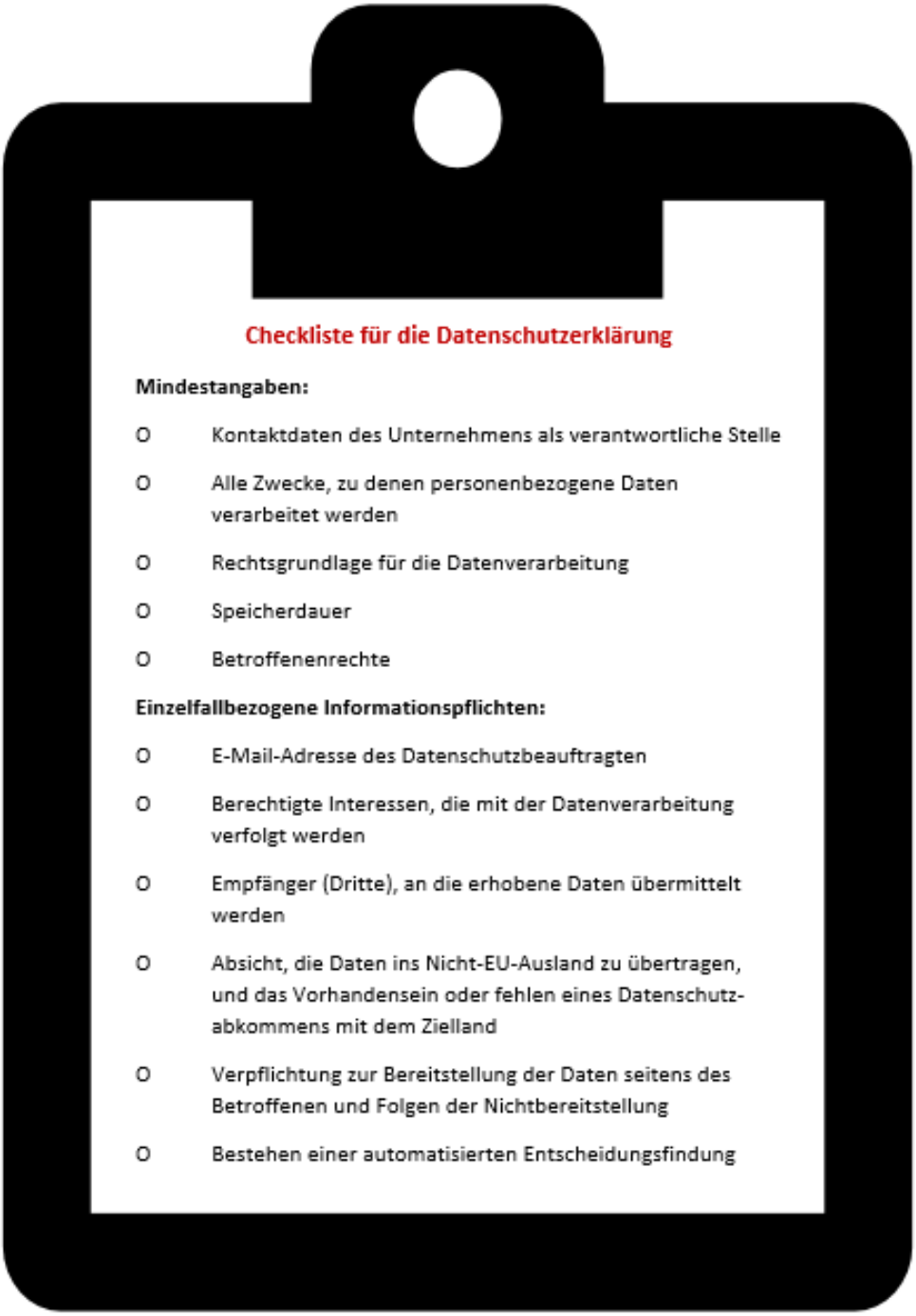
Einwilligung des Betroffenen	*Jeder Kunde wird auf die Erfassung der Daten durch die Mitarbeiter mündlich hingewiesen und darauf aufmerksam gemacht, dass er diese Daten jederzeit einsehen und löschen lassen kann.*

2. Bewerberdaten

Verantwortlich	*Geschäftsführerin Gerda Gehalt, Adresse, Telefonnummer*
Zweck	*Bewerbermanagement*
Betroffene	*Bewerber*
Wer kann auf die Daten zugreifen?	*Geschäftsführerin Gerda Gehalt, Ausbildungsleiterin Dieter Dienst*
Datenkategorie	*Bewerbungsmappen, Lebensläufe, Adressdaten (Name, Adresse, Telefonnummer, E-Mail-Adresse)*
Übermittlung an Drittstaaten	*Nein*
Löschfrist	*Sechs Monate nach Beendigung des Bewerbungsverfahrens*
Rechtsgrundlage	*Art. 13 Abs. 1 und Abs. 2 DSGVO*
Einwilligung des Betroffenen	*Bewerber werden mit einer automatischen E-Mail über den Zweck der Datenerhebung und die Dauer der Datenaufbewahrung informiert.*

Hinweis: *Darüber hinaus müssen Unternehmen den Weg der Daten nachzeichnen, von der Erhebung (Auftragsentgegennahme bei Arber) über die Speicherung (in diesem Fall in der Warenwirtschaft der Sage Applikation) bis hin zur Nutzung (zum Beispiel durch die Mitarbeiter).*

9.3 Checkliste zur Datenschutzerklärung



Checkliste für die Datenschutzerklärung

Mindestangaben:

- O Kontaktdaten des Unternehmens als verantwortliche Stelle
- O Alle Zwecke, zu denen personenbezogene Daten verarbeitet werden
- O Rechtsgrundlage für die Datenverarbeitung
- O Speicherdauer
- O Betroffenenrechte

Einzelfallbezogene Informationspflichten:

- O E-Mail-Adresse des Datenschutzbeauftragten
- O Berechtigte Interessen, die mit der Datenverarbeitung verfolgt werden
- O Empfänger (Dritte), an die erhobene Daten übermittelt werden
- O Absicht, die Daten ins Nicht-EU-Ausland zu übertragen, und das Vorhandensein oder fehlen eines Datenschutz-abkommens mit dem Zielland
- O Verpflichtung zur Bereitstellung der Daten seitens des Betroffenen und Folgen der Nichtbereitstellung
- O Bestehen einer automatisierten Entscheidungsfindung

10.0 Glossar

AO
Im Bereich des Steuerrechts werden die Aufbewahrungspflichten in der Abgabenordnung (AO) geregelt.

Aufsichtsbehörde(n)

ist/sind die vom jeweiligen Mitgliedstaat eingerichtete(n) Behörde(n), die der unabhängigen Datenschutzaufsicht dienen und die Einhaltung der DSGVO überwachen sollen.

Auftragsverarbeiter
ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Auftragsverarbeitung
ist die Verarbeitung personenbezogener Daten durch externe Dienstleister für den Auftraggeber (z. B. den Online-Händler).

BAO (AT)

Im Bereich des Steuerrechts werden die Aufbewahrungspflichten in der Bundesabgabenordnung (BAO) geregelt.

BDSG
Das Bundesdatenschutzgesetz regelt zusammen mit den Datenschutzgesetzen der Länder und anderen bereichsspezifischen Regelungen den Umgang mit personenbezogenen Daten, die in Informations- und Kommunikationssystemen oder manuell verarbeitet werden. Es setzt die Datenschutzrichtlinie um, die durch die DSGVO aufgehoben und ersetzt wird.

Betroffener
ist die Person, deren persönliche Daten berührt werden.

Code of conduct
sind Verhaltensregeln für den Umgang mit personenbezogenen Daten, die von den Aufsichtsbehörden genehmigt werden, insbesondere Anleitungen, wie der Verantwortliche oder Auftragsverarbeiter die Datenverarbeitung durchzuführen hat und wie die Einhaltung der Anforderungen nachzuweisen ist.

Datenübertragbarkeit/Datenportabilität
ist der Anspruch einer Person, eine Kopie der sie betreffenden personenbezogenen

Daten in einem üblichen und maschinenlesbaren Dateiformat zu erhalten. Der Nutzer hat damit das Recht, Daten von einem Anbieter zu einem anderen „mitzunehmen".

Datensicherheit
bedeutet, dass der Verantwortliche unter Berücksichtigung des Stands der Technik oder dem Zweck der Datenverarbeitung geeignete Maßnahmen umzusetzen hat, um die Sicherheit der Daten zu gewährleisten (z. B. Verschlüsselung, Passwörter).

Datensparsamkeit
bedeutet, dass die Datenverarbeitung auf das notwendige Maß beschränkt sein muss, beispielsweise bei einer Bestellung im Online-Shop nur die Anschrift angefragt werden darf und nicht das Geschlecht.

Datenverarbeitung
ist jeder Vorgang im Zusammenhang mit personenbezogenen Daten wie

- *Erheben*
- *Erfassen*
- *Organisation*
- *Ordnen*
- *Speicherung*
- *Anpassung oder Veränderung*
- *Auslesen*
- *Abfragen*
- *Verwendung*
- *Offenlegung durch Übermittlung, Verbreitung oder Bereitstellung*
- *Abgleich oder die Verknüpfung*
- *Einschränkung*
- *Löschung*
- *Vernichtung*

Drittstaaten
sind Länder, die weder der Europäischen Union angehören noch zu den Staaten des Europäischen Wirtschaftsraumes zählen.

DSG (AT)

Die Datenschutz-Grundverordnung ist zwar als EU-Verordnung im jeden EU-Mitgliedstaat unmittelbar anwendbar, sie enthält jedoch zahlreiche Öffnungsklauseln und lässt dem nationalen Gesetzgeber gewisse Spielräume. Zur Durchführung dieser Öffnungsklauseln und Spielräume wurde in Österreich das „Datenschutz-Anpassungsgesetz 2018", eine Novelle des DSG 2000 (künftig: DSG) beschlossen.

DSGVO

Datenschutzgrundverordnung, die ab 05/2018 in Kraft tritt und eine Modernisierung und Anpassung der bestehenden Datenschutzregelungen in den EU-Mitgliedsstaaten regelt.

Einwilligung der betroffenen Person
ist jede unmissverständlich abgegebene Erklärung oder eindeutige Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden Daten einverstanden ist.

Folgenabschätzung
ist die Abschätzung der Folgen für den Schutz personenbezogener Daten und muss durchgeführt werden, wenn die Datenverarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten birgt.

GDPR
General Data Protection Regulation – englische Bezeichnung der DSGVO.

Kohärenzverfahren
ist die Befugnis des Europäischen Datenschutzausschusses, im Falle von Unstimmigkeiten zwischen den Aufsichtsbehörden verbindliche Beschlüsse zu treffen, um die ordnungsgemäße und einheitliche Anwendung der DSGVO sicherzustellen.

Marktortprinzip
besagt, dass ausländische Unternehmen nur dann Zugang zum europäischen Markt erhalten, wenn sie sich an die hier geltenden Regelungen halten.

One-Stop-Shop
heißt, dass sich Unternehmen, die Niederlassungen in mehreren EU-Staaten haben und dort Daten verarbeiten, bei grenzüberschreitender Datenverarbeitung nur an die Aufsichtsbehörde an ihrem Hauptsitz wenden können.

Personenbezogene Daten
sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen; als identifizierbar wird eine Person angesehen, die direkt oder indirekt mittels Zuordnung zu einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann.

Privacy by Default (Dt.: Datenschutz durch Voreinstellung)
bedeutet, dass Produkte standardmäßig datenschutzfreundlich eingestellt sind (z. B. datenschutzfreundliche Voreinstellung eines Internet-Browsers). Hintergrund dieser Regelung ist, dass viele Nutzer nicht über ausreichende IT Kenntnisse verfügen und somit keine Einstellungen zum Schutz ihrer personenbezogenen Daten vornehmen

können. Darüber hinaus muss dem Nutzer Funktionalitäten zur Verfügung gestellt werden, mit denen er seine Privatsphäre schützen kann (z.B. Verschlüsselung).

Privacy by Design (Dt.: Datenschutz durch technische Konstruktion)
bedeutet, dass Unternehmen schon bei der Entwicklung und Konzeption ihrer (internen) Prozesse und Produkte (z. B. einer Software) dem Datenschutz und der DSGVO Rechnung tragen müssen. Es soll vorgebeugt werden, dass die Vorgaben nach dem Datenschutz und Datensicherheit erst nach dem Bereitstellen von IT-Systemen durch teure und zeitaufwendige Zusatzprogrammierungen umgesetzt werden. Bereits bei der Herstellung sollten Möglichkeiten wie Deaktivierung von Funktionalitäten, Anonymisierung oder Pseudonymisierung aber auch an Authentisierung und Authentifizierung oder Verschlüsselungen berücksichtigt werden.

Profiling
ist jede automatisierte Verarbeitung personenbezogener Daten, um bestimmte personenbezogene Aspekte zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser Person zu analysieren oder vorherzusagen.

Pseudonymisierung
ist die die Anonymisierung von personenbezogenen Daten in einer Weise, dass diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

Sensible Daten
sind personenbezogene Daten, aus denen die rassische und ethische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung, Daten über Gesundheit oder Sexualleben und sexuelle Ausrichtung.

Verantwortlicher
ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Verarbeitung von personenbezogenen Daten entscheidet und für die Einhaltung der DSGVO sorgen muss.

Verarbeitungsverzeichnis
katalogisiert die Datenverarbeitungsprozesse.

Vorabkontrolle
ist die Prüfung von Datenverarbeitungsvorgängen