

DSGVO

Umsetzung in Sage Business Cloud Buchhaltung in Bezug auf EU- Datenschutzrecht

Sage Kunden, bzw. deren Unternehmen sind als Eigentümer der Daten für die Einhaltung der Pflichten zur EU-DSGVO selbst verantwortlich. Die Softwarelösungen von Sage in der jeweils aktuellsten, unter Wartung befindlichen Version (bestehender Softwarepflege- und Nutzungsvertrag vorausgesetzt) können Sage Kunden lediglich dabei unterstützen, die Anforderungen der EU-DSGVO zu erfüllen.

Sage hat für Fragen speziell zur DSGVO eine E-Mail-Adresse eingerichtet: DSGVO@sage.de. Bitte beachten Sie, dass Sie hierüber keine rechtliche Beratung erhalten.

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

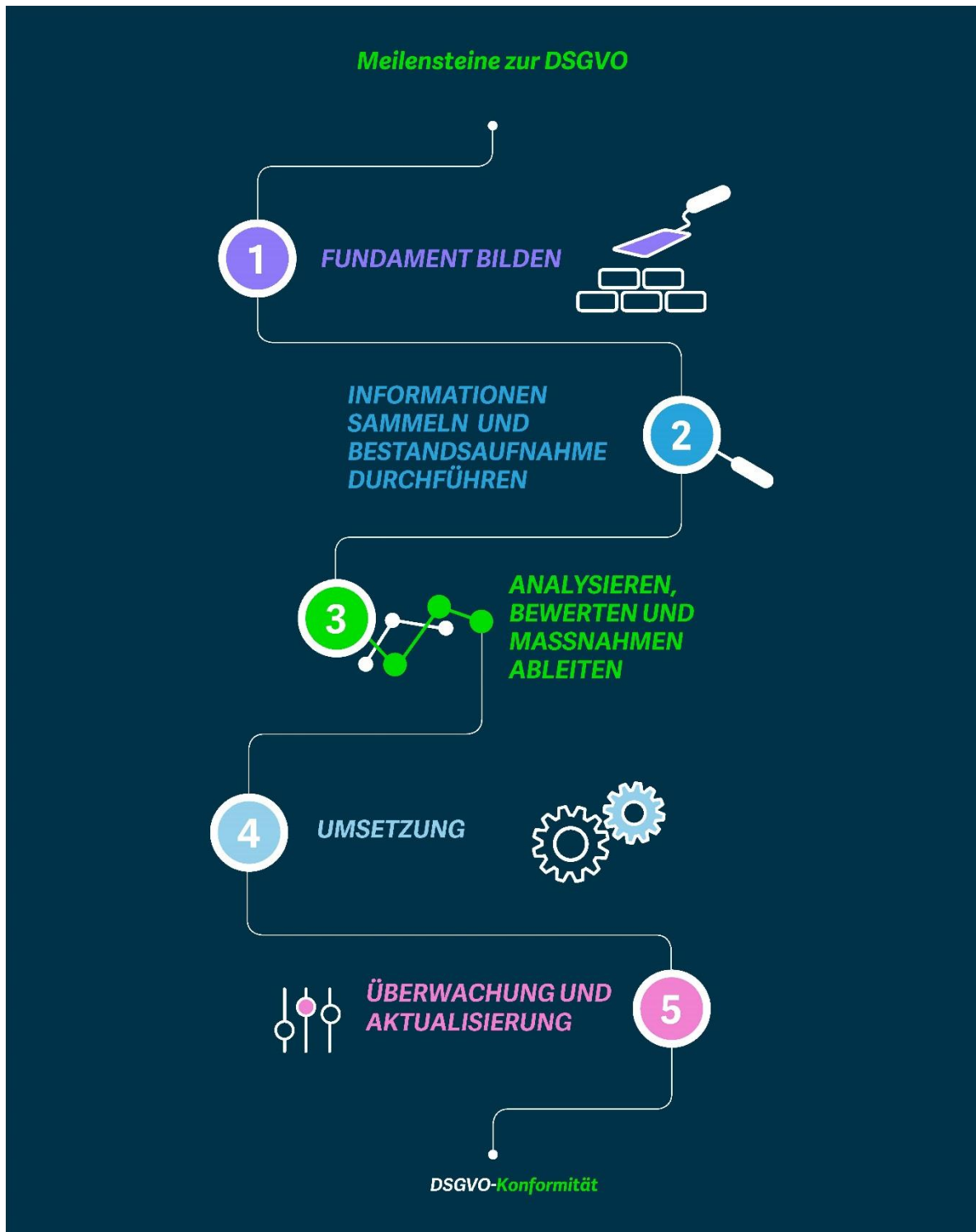
Inhaltsverzeichnis

1.0	Meilensteine zur DSGVO	4
2.0	Datenschutzgrundverordnung (DSGVO)	7
2.1	Geltungsbereich der DSGVO	7
2.2	Pflichten, die sich aus der DSGVO ergeben	9
2.3	Rechte die sich aus der DSGVO ergeben	9
2.4	Maßnahmen zur Datensicherheit	10
2.5	Konsequenzen bei Nichteinhaltung	11
2.6	Stellen Sie sicher, dass Ihre Datenschutzrichtlinien aktuell sind	11
2.7	Im Unternehmen können folgende persönliche Daten verarbeitet werden	11
2.8	Fragestellungen, um die Umsetzung der DSGVO zu gewährleisten	12
3.0	Maßnahmen zum Datenschutz in der Sage Applikation	13
3.1	Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person (Artikel 12)	13
3.2	Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Artikel 13)	13
3.3	Informationspflicht wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Artikel 14)	14
3.4	Auskunftsrecht der betroffenen Person (Artikel 15)	14
3.4.1	Wie gehen Sie vor, wenn Sie nach personenbezogenen Daten suchen?	14
3.4.2	Wie erfahren Sie, wie lange Sie Daten noch aufbewahren müssen?	16
3.4.3	Wie finden Sie heraus, was für eine Beziehung Sie zu einer Person haben?	16
3.5	Recht auf Berichtigung (Artikel 16)	16
3.5.1	Wie gehen Sie vor, wenn Sie personenbezogene Daten in Ihrem Sage Programm korrigieren, überschreiben oder ändern möchten?	17
3.6	Recht auf Löschung (Artikel 17)	17
3.6.1	Wie können Sie Stammdaten in Ihrem Sage Programm löschen?	17
3.6.2	Wie können Sie Bewegungsdaten in Ihrem Sage Programm löschen?	18

3.7	Recht auf Einschränkung der Verarbeitung (Artikel 18)	19
3.7.1	Wie können Sie den Status aktiv/inaktiv bei personenbezogenen Daten hinterlegen?	19
3.8	Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung (Kapitel 19)	19
3.9	Recht auf Datenübertragbarkeit (Artikel 20)	19
3.9.1	Vorgehensweise beim Datenexport aus Ihrer Sage Applikation	20
3.10	Widerspruchsrecht (Artikel 21)	20
3.11	Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (Artikel 22)	20
3.12	Verantwortung des für die Verarbeitung Verantwortlichen (Artikel 24)	20
3.12.1	Wie richten Sie eine Benutzer- und Rechteverwaltung in Ihrem Sage Programm ein?	21
3.13	Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Artikel 25)	21
3.14	Auftragsverarbeiter (Artikel 28)	21
3.15	Allgemeine Grundsätze der Datenübermittlung (Artikel 44)	22

1.0 Meilensteine zur DSGVO

Sage hilft Ihnen, damit Sie die wichtigsten Wegpunkte und Maßnahmen bei der Umsetzung zur EU-DSGVO in Ihrem Unternehmen umsetzen können.



1. *Fundament bilden*
 - a. *Sensibilität und Aufmerksamkeit im Unternehmen schaffen*
 - b. *Informationen zur DSGVO sammeln und studieren (Leitfäden, Checklisten, Auslegungshilfen)*
 - c. *Prioritäten für verschiedene Themen bestimmen*
 - d. *Notwendige Ressourcen festlegen und organisieren*
 - e. *Projekt- und ggf. Führungsstruktur einrichten und Teams bilden*
2. *Informationen sammeln und Bestandsaufnahme durchführen*
 - a. *Datenverarbeitungsaktivitäten untersuchen (welche Daten werden wie lange und aus welchem Grund gespeichert)*
 - b. *Gegenwärtige Datenschutzmaßnahmen und die dahinterstehenden Prozesse identifizieren und evaluieren*
 - c. *Veränderungen der Datenverarbeitungsaktivitäten verfolgen*
 - d. *Technische Ressourcen in Bezug auf Verschlüsselungs- und Sicherheitsmechanismen überprüfen*
3. *Analysieren, Bewerten und Maßnahmen ableiten*
 - a. *Informationen aus Schritt 2 auswerten*
 - b. *Lücken und Schwachstellen bestimmen und daraus Maßnahmen ableiten*
 - c. *Spielräume ausloten: Bereiche bestimmen, in denen:*
 - d. *die Vorgaben der DSGVO weniger streng sind als bisher*
 - e. *Projektplan zum Erreichen der DSGVO-Konformität erstellen*
4. *Umsetzung*
 - a. *Neue Datenzugriffs- und Datenaufbewahrungsprozesse erarbeiten*
 - b. *Notwendige technische Änderungen vornehmen*
 - c. *Verantwortlichkeiten (neu) zuteilen und die entsprechenden Mitarbeiter schulen*
 - d. *Prozesse zur Umsetzung verfahrensmäßiger DSGVO-Vorgaben etablieren*
 - e. *Verträge, Einwilligungen und sonstige Dokumente im Sinne der DSGVO überarbeiten*

Erfahren Sie im [Sage Video](#) mehr zum Thema DSGVO oder nutzen Sie die [Schulungsangebote](#) rund um das Thema Datenschutz aus unserer Sage Academy.

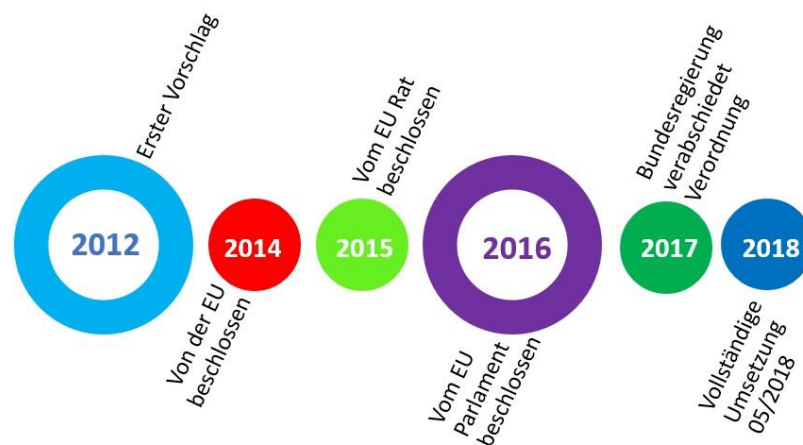
Weiterführende Informationen finden Sie unter:

- *FAQ zur DSGVO beinhaltet zusätzlich unterschiedliche Checklisten*
- *Übersicht der Aufbewahrungsfristen*
- *Mustervorlage eines Auftragsvertrags*
- *Musterverzeichnis von Verarbeitungstätigkeiten*
- *Mustervorlage zur Mitteilung einer Datenschutzverletzung an die Datenschutzaufsichtsbehörde*
- *Fragebogen zur Umsetzung der DSGVO*
- *Muster zur Auskunftserteilung*
- *Mustervorlage technische und organisatorische Maßnahmen (TOM)*
- *Informationsschreiben des Bundesfinanzministeriums zur DSGVO*
- *FAQ des DMS Herstellers d.velop*
- *FAQ des Webshop Anbieters ePages*

Eine detaillierte Beschreibung zu allen Artikeln der DSGVO-Verordnung finden Sie unter www.dsgvo-gesetze.de

2.0 Datenschutzgrundverordnung (DSGVO)

Ab 25. Mai 2018 gilt in ganz Europa ein neues Datenschutzrecht. Die EU-Datenschutz-Grundverordnung (DSGVO) oder GDPR (General Data Protection Regulation), die am 4. Mai 2016 im Europäischen Amtsblatt veröffentlicht wurde, löst die alte Richtlinie aus 1995 ab. An diese Richtlinie müssen sich nicht nur Unternehmen mit Sitz in der EU halten, sondern auch alle Unternehmen außerhalb der EU, die EU-Bürgern Produkte oder Dienstleistungen anbieten oder ihr Verhalten beobachten.



Mit der DSGVO erhalten Einzelpersonen mehr Kontrolle über ihre personenbezogenen Daten. Die neue Regelung sorgt für mehr Transparenz bei der Nutzung von Daten und erhöht die Sicherheit zum Schutz Ihrer Daten.

DSGVO betrifft Sie NICHT, wenn:

Sie beispielsweise eine Geburtstagsliste privat aufbewahren und nur für sich verwenden. Sobald Sie diese jedoch mit anderen teilen (z.B. via Social Media), fällt diese Geburtstagsliste unter die DSGVO.

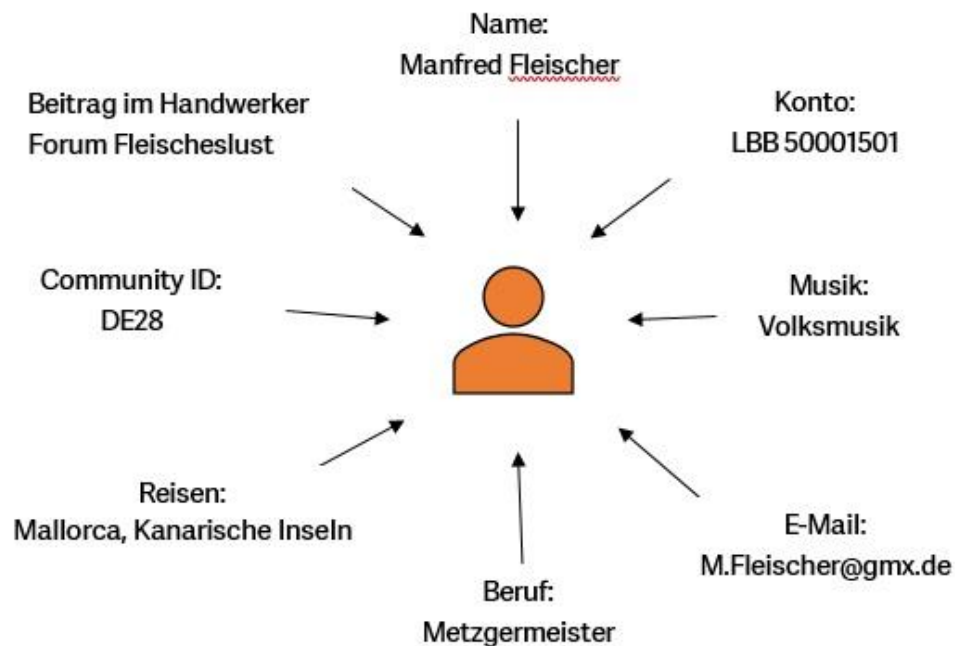
DSGVO betrifft Sie, wenn:

Sie personenbezogene Daten im EU-Wirtschaftsraum nutzen. Hierzu regelt die DSGVO deren Umgang und die Sicherheit mit den Daten, die auf eine Person zurückzuführen sind. Schützen Sie sensible Daten beispielsweise durch Verschlüsselung!

2.1 Geltungsbereich der DSGVO

Der Geltungsbereich der DSGVO betrifft alle Unternehmen, Behörden, gemeinnützige und andere Organisationen, die Waren und Dienstleistungen an Personen in der Europäischen Union (EU) verkaufen beziehungsweise Daten von EU-Bürgern erfassen und sammeln.

Einzelangabe zu persönlichen und sachlichen Verhältnissen
einer bestimmten natürlichen Person



Persönliche Daten gemäß Verordnung sind beispielsweise:

- Vor- und Zuname
- Anschrift
- Familienstand
- Geburtsdatum
- E-Mail-Adressen
- Telefonnummer (Anschlussinhaber)
- Personalausweisnummer
- Sozialversicherungsnummer
- Rentenversicherungsnummer
- KFZ-Kennzeichen (Autoinhaber)
- Positionsdaten
- Benutzerkonto (+Dienst)
- Social Media Posts
- IP Adressen
- Cookies
- Medizinische Informationen
- Bild/Video einer oder mehrerer Personen
- Unterschrift
- Bank Details (Konto/Kreditkarten)
- Vorstrafen
- Genetische Daten /Krankendaten
- Werturteile wie z.B. Zeugnisse
- Körperliche Merkmale/ Geistige Zustände
- Zugfahrkarte (siehe Beispiel)

Beispiel Zugfahrkarte: Wird der Käufer während des Erwerbs einer Fahrkarte von einer Sicherheitskamera gefilmt, nutzt zum Bezahlen ein elektronisches Zahlungsmittel und wurde das Ticket personalisiert, muss bei einem Zugticket von

„personenbezogenen Daten“ ausgegangen werden. Gleiches gilt für das verwendete IT-System.

2.2 Pflichten, die sich aus der DSGVO ergeben

- *Datenschutz als Grundbaustein*
- *Datenschutzfreundliche Voreinstellungen*
- *Pseudonymisierung & Verschlüsselung personenbezogener Daten*
- *Benennung eines Datenschutzbeauftragten, der die Einhaltung der Bestimmungen überwacht*
- *Einführung und Implementierung geeigneter Richtlinien und Prozesse (um die Einhaltung zu gewährleisten)*
- *Information über Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde innerhalb von 24 Stunden*
- *Verhinderung von unbefugtem Zugriff auf personenbezogene Daten*

2.3 Rechte die sich aus der DSGVO ergeben

- *Auskunftsrecht über Zweck und Rechtsgrundlage der Verarbeitung*
- *Einfordern der Löschung von Daten, wenn der Verarbeitungszweck erfüllt ist, Frist innerhalb eines Monats*
- *Transfer von verarbeiteten Daten zu einem anderen Unternehmen*
- *Recht auf Richtigstellung von Informationen*



2.4 Maßnahmen zur Datensicherheit

Für die Datensicherheit bei der Verarbeitung von personenbezogenen Daten gelten u.a. folgende Maßnahmen:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten (z.B. Passwortsicherungen von Dateien);
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen (z.B. Zutritts-/Zugangskontrollen, Zugriffsbeschränkungen). Dazu gehört auch, dass unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten („Auftragsprinzip“);
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (z.B. Backup-Programme);
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (z.B. Selbstevaluierungsprozesse).
- Es sind die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere bei unbeabsichtigter oder unrechtmäßiger Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugang zu personenbezogenen Daten („risikobasierter Ansatz“).
- Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens kann als Faktor herangezogen werden, um die Erfüllung der genannten Maßnahmen nachzuweisen.
- Zum Schutz der personenbezogenen Daten haben die Verantwortlichen und die Auftragsverarbeiter u.a. auch die Grundsätze des Datenschutzes durch Technik (privacy by design) und durch datenschutzfreundliche Voreinstellungen (privacy by default) zu berücksichtigen und geeignete interne Strategien festzulegen sowie entsprechende Maßnahmen zu setzen.



2.5 Konsequenzen bei Nichteinhaltung

Bei Verstößen sind drastische Strafen möglich:

- bis zu 20 Mio €
- oder Umsatzstrafen in Höhe von 4% des weltweiten Firmenumsatzes

2.6 Stellen Sie sicher, dass Ihre Datenschutzrichtlinien aktuell sind

- Fokussieren Sie die DSGVO-Forderung nach Transparenz
- Stellen Sie sicher, dass Ihre Datenschutzpolicies dies widerspiegeln.
- Beachten Sie die Auswirkungen von Interaktionen mit externen Datenverarbeitern und Lieferanten, die in ihrem Auftrag tätig sind.

Wichtig: Die Wahrung der Privatsphäre steht im Mittelpunkt aller Policies zur DSGVO.

2.7 Im Unternehmen können folgende persönliche Daten verarbeitet werden

- Kundendatenbanken
- Feedback Formulare
- E-Mails
- Fotos
- Überwachungsvideos
- HR-Datenbanken

- *Logfiles*
- *Backup/Archive*
- *Mitarbeiterzeiten*

2.8 Fragestellungen, um die Umsetzung der DSGVO zu gewährleisten

- *Speichern Sie nur die notwendigen Daten und werden diese auch nicht länger als notwendig gespeichert? (Aufbewahrungsfristen)*
- *Können wir sicherstellen, dass die Daten nur für einen spezifischen Zweck gespeichert und nicht anderweitig genutzt werden?*
- *Haben wir einen Prozess, um Personen Auskunft über ihre personengebundenen Daten zu geben?*
- *Haben Sie einen Prozess, um personenbezogene Daten auf Anforderung zu löschen?*
- *Werden die Daten an einem, für nicht jeden zugänglichen, sicheren Ort gespeichert?*
- *Sind Ihre gespeicherten personenbezogenen Daten ausreichend gegen Missbrauch geschützt?*
- *Kennen Sie die Haftungsrisiken und die veranschlagten Bußgelder bei Nicht-Einhaltung der DSGVO?*
- *Ist Ihr Budget zur Umsetzung der neuen Regelungen ausreichend bemessen?*
- *Haben Sie einen Datenschutzbeauftragten mit der erforderlichen Fachkenntnis, um die Neuerungen der DSGVO umzusetzen?*
- *Haben Sie Vereinbarungen zum Datenschutz mit Ihren Lieferanten, Kunden oder Mitarbeitern getroffen?*

3.0 Maßnahmen zum Datenschutz in der Sage Applikation

Die EU-Datenschutz-Grundverordnung bringt einige Veränderungen für den bisherigen Datenschutz. Die DSGVO-Pflichten sind dafür gedacht, dem Einzelnen mehr Rechte bezüglich seiner personenbezogenen Daten einzuräumen, die von ihm gespeichert sind.

In diesem Kapitel erläutern wir Ihnen ausgewählte Artikel der DSGVO. Wir geben Ihnen – soweit zutreffend - zu jedem Artikel Beispiele aus der Sage Applikation an die Hand, damit Sie geeignete Maßnahmen in der praktischen Umsetzung erhalten. Mit diesen Maßnahmen können Sie u.a. erreichen, dass Sie auf die Veränderungen gut vorbereitet sind.

3.1 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person (Artikel 12)

Diese Regelung betrifft jeden, der personenbezogene Daten verarbeitet. Es geht darum, die sogenannten Betroffenen (Kunden, Lieferanten, Interessenten, Vertreter oder Mitarbeiter etc.) zu informieren, wie Sie ihre Rechte ausüben können, die wir im Kapitel 2.3 aufgezählt haben. Diese Anforderung ist weitgehend unabhängig davon, welche IT-Systeme Sie einsetzen. Es handelt sich um eine Aufgabe, die Sie organisatorisch lösen müssen. Daher kontaktieren Sie bitte Ihren Datenschutzbeauftragten oder einen anderen Fachmann im Datenschutzrecht, um die bei Ihnen erforderlichen Maßnahmen zu erarbeiten.

3.2 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Artikel 13)

Auch hierbei handelt es sich um eine Anforderung, die organisatorisch zu lösen ist. Personenbezogene Daten können auf verschiedene Weise bei einem Betroffenen erhoben werden. Auf einer Webseite des Unternehmens können Kontaktdaten für einen Newsletter eingegeben werden. Es kann für Kunden eine telefonische Auftragserfassung geben bzw. man bestellt einfach per E-Mail. Oder eine Person bewirbt sich bei Ihnen auf einem Online-Portal für eine offene Stelle. Diese drei Beispiele zeigen, wie unterschiedlich die Wege sein können, wie ein Unternehmen personenbezogene Daten von Betroffenen erhalten kann. Für jeden Prozess, der dazu führt, dass in Ihren IT-Systemen die Daten einer Person gespeichert werden, müssen Sie sich überlegen, wie Sie Ihrer Informationspflicht aus §13 nachkommen. Gewöhnlich wird ein Unternehmen dieser Anforderung auf seiner Webseite und in seinen allgemeinen Geschäftsbedingungen nachkommen. Daher kontaktieren Sie bitte hierzu Ihren Datenschutzbeauftragten oder einen anderen Fachmann im Datenschutzrecht, um die bei Ihnen erforderlichen Maßnahmen zu erarbeiten.

3.3 Informationspflicht wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Artikel 14)

Analog dem eben beschriebenen, gelten die Informationspflichten auch für jene Fälle, in denen Sie die personenbezogenen Daten nicht selbst erheben, sondern aus einer dritten Quelle beziehen. In diesen Fällen ist es eigentlich zwingend, Ihren Datenschutzbeauftragten oder einen anderen Fachmann im Datenschutzrecht in die Beurteilung dieses Sachverhalts einzubeziehen.

3.4 Auskunftsrecht der betroffenen Person (Artikel 15)

Bei der Erfüllung dieser Anforderung der DSGVO kann Sie unsere Software unterstützen. Denn um einen Betroffenen zu informieren, was Sie an Daten von ihm gespeichert haben, sollten Sie auch jene Daten abfragen, die in Ihrem Sage Programm gespeichert sind. Dazu können Sie über die Suchfunktion in unserer Software die betroffene Person identifizieren. Wie das funktioniert, beschreiben wir in den folgenden Unterkapiteln.

Weiterhin kann Ihnen unser Programm die Information liefern, zu welchem Zweck die Daten der Person erfasst worden sind (z.B. Beginn der Kunden- oder Lieferantenbeziehung) und wie lange diese Daten noch aufzubewahren sind (z.B. 6 Jahre wg. Aufbewahrungspflicht einer Rechnung lt. Abgabenordnung).

Bitte beachten Sie, dass das Auskunftsrecht ausschließlich für natürliche Personen gilt. Auch sollten Sie darauf achten, dass Sie nicht die Rechte und Freiheiten anderer Personen beeinträchtigen, wenn Sie z.B. Dokumente herausgeben. Diese könnten den Namen einer dritten Person beinhalten (z.B. Sachbearbeiter in einer Rechnung). Daher ist es unbedingt empfehlenswert, wenn Sie die Antwort auf ein Auskunftersuchen gemeinsam mit Ihrem Datenschutzbeauftragten oder einem anderen Fachmann im Datenschutzrecht erstellen.

3.4.1 Wie gehen Sie vor, wenn Sie nach personenbezogenen Daten suchen?

In Sage Business Cloud Buchhaltung werden personenbezogene Daten in folgenden Arbeitsbereichen abgespeichert:

- Unter Einstellungen (Zahnrad) -> Mein Profil
 - Vorname
 - Nachname
 - E-Mail-Adresse
- Unter Einstellungen (Zahnrad) -> Informationen zum Unternehmen
 - Firmenname
 - Adresszeile 1
 - Adresszeile 2
 - Stadt
 - Postleitzahl
 - Land
 - Webseite

- Telefonnummer
- Mobilfunknummer
- *Unter Kontakte -> Kunden -> Kontaktdetails*
 - Firmenname
 - Kontaktname
 - Referenz
 - E-Mail
 - Mobiltelefon
 - Telefonnummer
 - Straße und Hausnummer
 - Adresszusatz
 - Postleitzahl
 - Ort
 - Land
 - Steuernummer
 - Ust-ID
- *Unter Kontakte -> Kunden -> Lieferadresse*
 - Straße und Hausnummer
 - Adresszusatz
 - Postleitzahl
 - Ort
 - Land
- *Unter Kontakte -> Kunden -> Zahlungsinformationen*
 - Kontobezeichnung
 - BIC / Swift
 - IBAN
- *Unter Kontakte -> Lieferanten -> Kontaktdetails*
 - Firmenname
 - Kontaktname
 - Referenz
 - E-Mail
 - Mobiltelefon
 - Telefonnummer
 - Straße und Hausnummer
 - Adresszusatz

- Postleitzahl
- Ort
- Land
- Steuernummer
- Ust-ID
- Unter Kontakte -> Lieferanten -> Zahlungsinformationen
 - Kontobezeichnung
 - BIC / Swift
 - IBAN

Kunden- und Lieferantendaten werden jedoch weiterverarbeitet und die Suche nach allen Vorkommen von personenbezogenen Daten ist entsprechend komplexer. Zum Kunden können z.B. Dokumente, offene Posten und vieles mehr erfasst sein.

3.4.2 Wie erfahren Sie, wie lange Sie Daten noch aufbewahren müssen?

In dem beiliegenden Dokument „Aufbewahrungsfristen“ sehen Sie, wie lange bestimmte Dokumente aufbewahrt werden müssen. Sollten diese Fristen noch nicht erreicht sein, so dürfen Sie die Datensätze und die darin enthaltenen personenbezogenen Daten nicht löschen.

Ebenso können betriebswirtschaftliche Gründe gegen ein Löschen der Daten sprechen. Solange z.B. noch nicht beglichene offene Posten des Kunden berechtigt im System vorhanden sind oder Belege im System vorhanden sind, so können und dürfen die personenbezogenen Daten nicht gelöscht werden.

Unter „Einstellungen -> Finanz- und Steuereinstellungen“ können Sie die Aufbewahrungszeit individuell einstellen.

3.4.3 Wie finden Sie heraus, was für eine Beziehung Sie zu einer Person haben?

Sie können die Beziehung über den jeweiligen Kontext (als was ist eine Person gespeichert) herausfinden. Beispielsweise können Mitarbeiter sowohl unter den Benutzern der Rechteverwaltung, als auch unter den Kunden angelegt sein.

3.5 Recht auf Berichtigung (Artikel 16)

Diese Anforderung der DSGVO ist eine, die in Ihrem eigenen Interesse liegt. Es geht um aktuelle Daten zu einer Person. Wenn also jemand geheiratet und einen neuen Namen angenommen hat oder wenn sich Telefon, E-Mail oder die Wohnanschrift verändert haben, so darf die Person verlangen, dass Sie in Ihrem IT-Programm diese Angaben korrigieren. So eine Aktualisierung ist im beiderseitigen Interesse. Sie kann über die reinen Angaben zu Name und Anschrift hinausgehen, wenn z.B. unberechtigt eine Mahnung verschickt wurde. Eine solche Änderung dürfte in beiderseitigem Interesse sein.

3.5.1 Wie gehen Sie vor, wenn Sie personenbezogene Daten in Ihrem Sage Programm korrigieren, überschreiben oder ändern möchten?

Öffnen Sie bitte wie in 3.4.1 beschrieben den passenden Adressstamm und suchen Sie den zur Person gehörenden Datensatz. Sie können die zu ändernden Felder editieren und den Datensatz im Anschluss speichern.

3.6 Recht auf Löschung (Artikel 17)

Das Recht auf Löschung von Daten ist ein sehr weitreichendes Recht und es ist empfehlenswert, dieses unbedingt zu beachten. Sage empfiehlt Ihnen, für jedes Ihrer IT-Systeme, das personenbezogene Daten verarbeitet, sich ein Lösch-Konzept zu überlegen. Haben Sie ein solches und wenden es konsequent an, dürften Sie selten in die Verlegenheit kommen, von einem Betroffenen dazu aufgefordert zu werden, seine Daten zu löschen. Denn dann dürften Sie ohnehin den Grundsatz der Datensparsamkeit, der dem Datenschutzrecht innewohnt, befolgen.

Personenbezogene Daten dürften sich in den meisten Fällen nur dann in den IT-Systemen von Sage finden lassen, wenn es eine geschäftliche Beziehung zu der Person gibt. Die Daten von Kunden, Lieferanten, Vertretern und Mitarbeitern werden gewöhnlich nur zu diesem Zweck erfasst. Hier müssen Sie z.B. die gesetzlichen Aufbewahrungsfristen beachten, bevor Sie die Daten löschen. Aus diesem Grund sollten Daten nur gezielt gelöscht werden, z.B. ganze Geschäftsjahre nach dem Ablauf der Fristen. Eine weitere Option könnte sein, dass personenbezogene Daten anonymisiert werden. Dabei werden alle Informationen zu einer natürlichen Person mit einem Platzhalter (z.B. „*“ oder „#“) überschrieben. Wird dieses Vorgehen gewählt muss sichergestellt sein, dass die Daten nicht auf Umwegen wiederhergestellt werden können.

Wie Sie dabei vorzugehen haben, beschreiben wir in den folgenden Unterkapiteln.

3.6.1 Wie können Sie Stammdaten in Ihrem Sage Programm löschen?

Öffnen Sie bitte wie in 3.4.1 beschrieben den passenden Stammdatensatz und suchen Sie den zur Person gehörenden Datensatz. Unter „Einstellungen“ können Sie unter „DSGVO Personenbezogene Daten“ die Auswahl „Daten entfernen“ treffen.

Übersicht Einnahmen Ausgaben **Kontakte** Artikel & Dienstleistungen Bank & Kasse Manuelle Buchungen Berichte Einstellungen

OFFEN (0)
0,00 €

KREDITLIMIT
Nicht angegeben

ÜBERFÄLLIG (0)
0,00 €

ZAHLUNGSZIEL
30 Tage

EINNAHMEN SEIT JAHRESBEGINN BIS HEUTE (1)
1,5 Tsd. €

LETZTE EINNAHME
01.02.2017

JAHRESUMSATZ (1)
1,5 Tsd. €

DURCHSCHNITTSEINNAHMEN
1,5 Tsd. €

Herbert Meier
0305646984
herbert.maier@maierag.de
Teststraße 59, Berlin, 10000

Aktivitäten Kontakte und Adressen Zahlungsinformationen **Einstellungen** Notizen

Kontodetails

Firma/Name Meier AG

Referenz [Referenz hinzufügen](#)

Debitorennummer 10001

Standardpreis Verkaufspreis

Sprache Deutsch

Buchungskonto 8400 - Erlöse 19 % USt

Steuernummer [Steuernummer hinzufügen](#)

USt-ID [USt-ID hinzufügen](#)

Kundenauszüge BETA

Auszüge senden Ja

Kundenauszüge Postversand (PDF)

Empfänger Herbert Meier

Adresse Rechnungsadresse

DSGVO Persönliche Daten

Letztes Transaktionsdatum 02.02.2017

Vorgeschlagenes Datum zum Entfernen 01.04.2018

Verlangerte Frist Zum Entfernen 01.04.2018

Dieser Kontakt hat der Verwendung als permanenter Datensatz zugestimmt.

Daten entfernen Speichern Abbrechen

Deutsch © The Sage Group plc 2018

Da es eine Reihe von berechtigten Gründen (z.B. Kunde oder Lieferant ist in Belegen der Belegerfassung enthalten, Konto ist bereits bebucht) geben kann, warum der Datensatz nicht gelöscht werden darf, werden die personenbezogenen Daten aus diesem Datensatz durch diese Auswahl anonymisiert.

Übersicht Einnahmen Ausgaben **Kontakte** Artikel & Dienstleistungen Bank & Kasse Manuelle Buchungen Berichte Einstellungen

Kundendaten und Kontobewegungen. Unter dem Reiter „Kontakte und Adressen“ können Sie Kontaktdaten und Adressen anzeigen oder bearbeiten.

OFFEN (0)
0,00 €

KREDITLIMIT
Nicht angegeben

ÜBERFÄLLIG (0)
0,00 €

ZAHLUNGSZIEL
30 Tage

EINNAHMEN SEIT JAHRESBEGINN BIS HEUTE (1)
1,5 Tsd. €

LETZTE EINNAHME
01.02.2017

JAHRESUMSATZ (1)
1,5 Tsd. €

DURCHSCHNITTSEINNAHMEN
1,5 Tsd. €

DSGVO #1: Name
DSGVO #1: Telefonnummer
DSGVO #1: E-Mail
DSGVO #1: Straße, DSGVO #1: Ort, DSGVO: Postleitzahl

Aktivitäten Kontakte und Adressen Zahlungsinformationen **Einstellungen** Notizen

Kontodetails

Firma/Name DSGVO #1: Firma

Referenz [DSGVO #1 Beschreibung](#)

Debitorennummer 10001

Standardpreis Verkaufspreis

Sprache Deutsch

Buchungskonto 8400 - Erlöse 19 % USt

Steuernummer -

USt-ID DE DSGVO #1: USt-ID

Kundenauszüge BETA

Auszüge senden Ja

Kundenauszüge Postversand (PDF)

Empfänger DSGVO #1: Name

Adresse Rechnungsadresse

DSGVO Persönliche Daten

Persönliche Daten wurden entfernt 22.05.2018

Deutsch © The Sage Group plc 2018

3.6.2 Wie können Sie Bewegungsdaten in Ihrem Sage Programm löschen?

Bewegungsdaten können nur gelöscht werden, wenn zu ihnen keine weiteren Bewegungsdaten existieren d.h. wenn z.B. ein Angebot abgelaufen ist und zu keinem Auftrag geführt hat.

Um personenbezogene Daten aus einem Vorgang zu löschen bzw. zu anonymisieren, löschen Sie wie in 3.6.1 beschrieben die personenbezogenen Daten aus den entsprechenden Stammdaten. Die personenbezogenen Daten werden anschließend

automatisch aus allen - zum Stammdatensatz zugehörigen Vorgängen - entfernt. Bitte beachten Sie hierbei die jeweiligen Aufbewahrungsfristen.

Wenn Sie bereits seit längerer Zeit keine Bewegungsdaten mehr zu einer Person (Kunde/Lieferant) erfasst haben, empfehlen wir Ihnen einen neuen Datensatz anzulegen, so dass die alten personenbezogenen Daten, die ggf. nicht mehr aktuell sind, nach Ablauf der Aufbewahrungsfristen gelöscht werden können.

3.7 Recht auf Einschränkung der Verarbeitung (Artikel 18)

Unter bestimmten Umständen kann es für eine natürliche Person sinnvoll sein, statt die Löschung seiner Daten zu verlangen, nur deren Verarbeitung einzuschränken. Der Artikel 18 steht also im Zusammenhang mit Artikel 17. Hierzu ein Beispiel: Ein Kunde verlangt von Ihnen, seine personenbezogenen Daten zu löschen. Sie müssen ihm jedoch mitteilen, dass Sie aufgrund der Abgabenordnung, seine Daten noch für fünf Jahre aufbewahren müssen. Daraufhin kann der Betroffene von Ihnen verlangen, dass Sie seine Daten bis zu diesem Zeitpunkt aus Ihrer Verarbeitung herausnehmen. Sie sollten also ein Kennzeichen im Kundendatensatz hinterlegen, das Ihnen signalisiert, dass diese Daten gesperrt sind und nicht für Marketingmaßnahmen genutzt werden dürfen. Analog könnte dies bei Lieferanten oder ehemaligen Vertretern bzw. Mitarbeitern Ihres Unternehmens der Fall sein. Aber Achtung: Die Einschränkung der Verarbeitung entbindet Sie nicht von der Pflicht, die Daten nach Ablauf der Aufbewahrungsfristen oder des Anlasses zu dem die Verarbeitung eingeschränkt wurde, tatsächlich zu löschen.

Im nachstehenden Unterkapitel beschreiben wir, wie Sie vorgehen können, um ein solches Kennzeichen bei einem Datensatz zu hinterlegen.

3.7.1 Wie können Sie den Status aktiv/inaktiv bei personenbezogenen Daten hinterlegen?

Personenbezogene Daten können in Stammdaten enthalten sein. Stammdaten zu Kunden und Lieferanten können über die Option „Inaktiv“ im jeweiligen Stammdatensatz inaktiv bzw. aktiv gesetzt werden.

3.8 Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung (Kapitel 19)

Diese Anforderung betrifft Sie, falls Sie personenbezogene Daten Ihrer Kunden, Lieferanten, Vertreter, Mitarbeiter oder Bewerber mit Dritten geteilt haben. Es handelt sich um eine Aufgabe, die Sie organisatorisch lösen müssen. Daher kontaktieren Sie bitte Ihren Datenschutzbeauftragten oder einen anderen Fachmann im Datenschutzrecht, um die bei Ihnen erforderlichen Maßnahmen zu erarbeiten.

3.9 Recht auf Datenübertragbarkeit (Artikel 20)

Hierbei handelt es sich um das Recht eines Betroffenen seine personenbezogenen Daten, die er einem Dritten zur Verfügung gestellt hat, von diesem in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Diese Anforderung richtet sich vor allem an Service-Provider, die künftig den Umzug eines E-Mail-Postfachs oder eines Internet-Auftritts von einem Server zu einem anderen einfacher als bisher ermöglichen müssen. Bei klassischen on-premise-Produkten von Sage dürfte dieses Recht eher selten bis gar nicht zur Anwendung kommen, da sich die Daten bereits auf

einem lokalen Server befinden. Die Daten eines einzelnen Kunden, Lieferanten oder Mitarbeiter zu exportieren macht verhältnismäßig wenig Sinn, wenn gleich es doch möglich wäre. Cloud-Lösungen hingegen müssen diese Anforderung erfüllen. Im nachstehenden Unterkapitel beschreiben wir, wie ein Datenexport Ihrer Sage Anwendung vorgenommen werden kann bzw. wie Sie von uns einen solchen Datenexport erhalten, wenn Sie die Daten Ihrer Sage Lösung aus der Cloud von uns beziehen möchten.

3.9.1 Vorgehensweise beim Datenexport aus Ihrer Sage Applikation

Ihre Sage One Business Cloud Buchhaltung bietet Ihnen umfangreiche Möglichkeiten der Auskunftspflicht nachzukommen.

So können Sie z. B. im Stammdatenbereich den Bericht Kundenauszüge erstellen und in verschiedene Formate wie .csv oder .pdf exportieren.

3.10 Widerspruchsrecht (Artikel 21)

In diesem Kapitel der DSGVO geht es vor allem um eine Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung. Hiergegen kann eine Person Widerspruch einlegen. Da die Sage Produkte, vielleicht abgesehen von unserem Sage - CRM-System, nicht für Direktwerbung konzipiert bzw. funktional ausgelegt sind, dürfte dieses Thema, wenn überhaupt, nur einen sehr kleinen Teil unserer Anwender interessieren. Es handelt sich um eine Aufgabe, die Sie organisatorisch lösen müssen. Daher kontaktieren Sie bitte Ihren Datenschutzbeauftragten oder einen anderen Fachmann im Datenschutzrecht, um die bei Ihnen erforderlichen Maßnahmen zu erarbeiten, sollten Sie tatsächlich Direktwerbung betreiben.

3.11 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (Artikel 22)

Bei dieser Anforderung der DSGVO handelt es sich um einen Spezialfall. Sage Produkte beinhalten im Standardumfang keine Funktionen, die aufgrund einer ausschließlich automatisierten Verarbeitung Entscheidungen zu Personen treffen, die diese in rechtlicher Weise betreffen. Ein sogenanntes Profiling ist nicht Teil unserer Lösungen. Es werden aber Verarbeitungen genutzt, um z.B. Gehaltsabrechnungen zu erstellen, Rechnungen bzw. Mahnungen zu erzeugen, oder um den Personaleinsatz in der Produktion zu planen usw., was aber aufgrund der bestehenden vertraglichen Beziehungen mit den Betroffenen (Arbeitsvertrag, Kaufvertrag usw.) laut der DSGVO in jedem Fall zulässig ist.

3.12 Verantwortung des für die Verarbeitung Verantwortlichen (Artikel 24)

Dieses Kapitel der DSGVO betrifft jeden unserer Kunden, der in seinen IT-Systemen personenbezogene Daten verarbeitet. Dabei müssen Sie abhängig von der Art, dem Umfang, den Umständen und dem Zweck der Verarbeitung sowie einer Risikobeurteilung für die Rechte und Freiheiten der Personen, deren Daten Sie verarbeiten, sogenannte technische und organisatorische Maßnahmen (TOM's) treffen, um die DSGVO einzuhalten. Ein Teilaspekt dieser TOM's kann z.B. sein, dass Sie die Rechteverwaltung in Ihrer Software nutzen, um nur bestimmten Mitarbeitern den Zugriff auf personenbezogene Daten zu gewähren. Im folgenden Unterkapitel erhalten Sie

Informationen, welche Möglichkeiten Sie haben, mit Ihrer Sage Anwendung eine Rechte- und Benutzerverwaltung einzurichten.

3.12.1 Wie richten Sie eine Benutzer- und Rechteverwaltung in Ihrem Sage Programm ein?

Die Benutzerverwaltung finden Sie in den Einstellungen.

Hier können Sie Benutzer über deren E-Mail-Adresse einladen und verschiedene Rechte vergeben, vom Lesezugriff bis hin zu Administratorrechten. Unter „Erweiterte Berechtigungen“ können Sie auch einzelne Bereiche pro Benutzer freigeben bzw. beschränken. In der Liste aller Nutzer können Sie über die „Mülltonne“ Nutzer auch wieder löschen.

3.13 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Artikel 25)

In diesem Abschnitt der DSGVO geht es um technische und organisatorische Maßnahmen (TOM's), die Sie als verantwortliche Stelle für die Datenverarbeitung treffen müssen. Sie sollen bewirken, dass die Datenschutzgrundsätze wie z.B. Datenminimierung eingehalten werden und die Rechte der Betroffenen wirksam geschützt sind. Eine Möglichkeit, wie die Sage Software Sie dabei unterstützen kann, wurde im vorherigen Kapitel beschrieben. Es ist empfehlenswert, dass Sie gemeinsam mit Ihren Datenschutzbeauftragten oder einem anderen Fachmann im Datenschutzrecht, Ihre IT-Umgebung vollständig analysieren und die erforderlichen Maßnahmen erarbeiten.

3.14 Auftragsverarbeiter (Artikel 28)

Das Thema Auftragsverarbeitung wird Ihnen im Zusammenhang mit Ihrem Sage Produkt u.a. in folgenden Fällen begegnen:

- Supportleistungen bzw. Hotline direkt durch Sage oder Ihren Business Partner
- Consulting oder Projektprogrammierung direkt durch Sage oder Ihren Business Partner
- Cloud-Lösungen von Sage

In den ersten beiden Fällen kann, im dritten Fall trifft es immer zu, dass Sie personenbezogene Daten Ihrer Kunden, Lieferanten, Vertreter, Mitarbeiter oder Interessenten etc. an einen Dritten weitergeben – an Sage oder Ihren Business Partner. Damit dies dem §28 DSGVO entsprechend erfolgen darf, müssen Sie zuvor eine Vereinbarung zur Auftragsverarbeitung mit Sage oder dem Business Partner abschließen. Dafür gibt es Vorlagen, die Sie von den genannten Parteien erhalten. Der wesentliche Inhalt einer solchen Vereinbarung besteht darin, dass der Auftragnehmer (Sage oder Ihr Business Partner) in Ihrem Auftrag und gemäß Ihren Weisungen, für einen bestimmten Zweck Ihre Daten verarbeitet. Ist die Aufgabe erledigt, löscht der Auftragnehmer gemäß Ihrer Anweisung die Daten. Die Daten bleiben zu jeder Zeit in Ihrem Besitz und werden zu keinem anderen Zweck verarbeitet, als zu dem, zu dem Sie den Auftragnehmer vertraglich verpflichtet haben.

Sollten Sie noch keine Vereinbarung abgeschlossen haben, empfehlen wir dringend, dies bis zum 25.05.2018 nachzuholen. Sage wird seine Business Partner und Kunden aktiv dazu auffordern, diese Vereinbarungen abzuschließen. Insbesondere dann, wenn Datenbanken an den Support gehen bzw. dem Professional Services übermittelt werden oder ein Cloud-Produkt von Sage im Einsatz ist.

Die Klärung der Vertragspartnerschaft hängt davon ab, mit wem Sie einen laufenden Support bzw. Hotline-Vertrag abgeschlossen haben bzw. wer Consulting oder Projektprogrammierung für Sie erbringt. Nutzen Sie eine Sage Cloud-Lösung, wird es Sage sein, mit dem Sie die Vereinbarung zu schließen haben.

Bitte kontaktieren Sie Sage unter dsgvo@sage.com, wenn Sie unsicher sind, wer Ihr Ansprechpartner für den Abschluss einer Vereinbarung zur Auftragsverarbeitung ist.

3.15 Allgemeine Grundsätze der Datenübermittlung (Artikel 44)

Mit Einführung der DSGVO gilt innerhalb der gesamten EU ein einheitliches Datenschutzrecht. Daher ist es unerheblich, in welchem Land der EU die personenbezogenen Daten, z.B. Cloud-Lösungen verarbeitet werden.

Sage hat sich aus grundsätzlichen Erwägungen (u.a. Abgabenordnung) dazu entschieden, fast alle Produkte, die in der Cloud angeboten werden, in Rechenzentren in Deutschland zu hosten. Somit erfolgt keine Werteübermittlung personenbezogener Daten in ein Drittland.

Einzelheiten zu den Orten der Datenverarbeitung und den Sublieferanten, mit denen Sage zusammenarbeitet, entnehmen Sie bitte der Vereinbarung zur Auftragsverarbeitung bzw. Ihrem Nutzungsvertrag für Ihre Cloud-Lösung.