DIE UHR TICKT:
DIE EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO) KOMMT!

2 | Wie Sie Ihr Unternehmen jetzt auf die neuen Datenschutzgesetze vorbereiten sollen

Inhaltsangabe

Kapitel 1

Ab dem 25. Mai 2018 wird es ernst

Ab dem 25. Mai 2018 gilt die neue Datenschutzgrundverordnung der Europäischen Union (EU-DSGVO). Sie konkretisiert viele schon bisher geltenden Normen, harmonisiert die nationalen Datenschutzgesetze und verschärft einige Tatbestände, die die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten betreffen. Die deutsche Bundesregierung hat die EU-DSGVO in nationales Recht umgesetzt und das seit 1977 existierende Bundesdatenschutzgesetz (BDSG) novelliert, das ebenfalls ab dem 25. Mai 2018 von allen Unternehmen in den Mitgliedsstaaten der EU anzuwenden ist. Darüber hinaus unterstehen ebenso alle Unternehmen weltweit der EU-DSGVO, wenn sie innerhalb der EU Waren oder Dienstleistungen anbieten und vermarkten wollen. Das bedeutet, dass auch ein Unternehmen aus den USA, das hier Produkte über einen Online-Shop anbietet, die europäischen Normen anwenden muss.

Sicherlich wird nicht alles so heiß gegessen, wie es in den Medien zurzeit dargestellt wird. Und natürlich schrecken die neuen Sanktionen erst einmal ab. Immerhin kann die EU bei Verstößen gegen die EU-DSGVO ein Bußgeld bis zu vier Prozent des Jahresumsatzes, maximal aber 20 Millionen Euro pro Verstoß verhängen. Aber die Unternehmen, die bisher eine BDSG-konforme Datenverarbeitung betrieben haben, müssen diese lediglich anpassen. Allerdings kann dies im Einzelfall recht aufwendig sein.

Mehr Informationen

1.1 Erst 13 Prozent haben Maßnahmen eingeleitet

Wenn Sie als Geschäftsführer, CIO, HR-Manager oder Leiter des Finanz- und Rechnungswesens bisher noch keine Maßnahmen zur Umsetzung der EU-DSGVO eingeleitet haben, sollten Sie jetzt damit starten. Allerdings sind Sie in guter Gesellschaft, wenn Sie noch nichts unternommen haben. Denn nach einer Umfrage des Branchenverbands Bitkom aus September 2017 ergab, dass bis dahin erst 13 Prozent der Unternehmen Maßnahmen eingeleitet hatten. Etwas alarmierend vermeldet der Internetverband, der großen „Mehrheit der Unternehmen in Deutschland" drohe in wenigen Monaten „Millionen-Bußgelder". Von den 13 Prozent meinen sogar nur 19 Prozent, dass sie mit der Umsetzung der neuen Bestimmungen in ihrem Betrieb bis zum Stichtag fertig würden. 55 Prozent der Befragten, die bereits angefangen haben, schaffen es nur teilweise, ihre Prozesse an die neuen Normen anzupassen.

„Die Zeit drängt, um die Vorgaben der Datenschutzgrundverordnung umzusetzen. Unternehmen, die bis jetzt abgewartet haben, müssen das Thema schnellstmöglich aufarbeiten", sagte Susanne Dehmel, Geschäftsleiterin Recht & Sicherheit bei der Bitkom. „Wer den Kopf in den Sand steckt, verstößt demnächst gegen geltendes Recht und riskiert empfindliche Bußgelder zu Lasten seines Unternehmens."

49 %

der deutschen Unternehmen beschäftigen sich bereits mit der EU-DSGVO

33 %

haben sich über die Verordnung noch gar keine Gedanken gemacht

Die größten Herausforderungen bei der Umsetzung der EU-DSGVO:

52 %

fürchten sich vor dem schwer abzuschätzenden Aufwand

43 %

haben Bedenken beim Thema Rechtssicherheit

32 %

sehen einen Mangel an praktischen Umsetzungshilfen

28 %

wünschen sich Auslegungshilfen für die Verordnung

27 %

hätten gerne Praxisleitfäden

16 %

wünschen sich Handreichungen von den Aufsichtsbehören

In diesem E-Book fassen wir für Sie die wichtigsten Regelungen der EU-DSGVO und des novellierten BDSG zusammen und geben Ihnen Tipps für die Umsetzung in Ihrem Unternehmen.

Mehr Informationen

Kapitel 2
Grundlagen der Datenschutzgesetze

Um die Neuerungen der EU-DSGVO und des BDSG zu verstehen, lohnt sich ein kurzer Exkurs in die Grundlagen des Datenschutzes. Denn alle Verschärfungen, Konkretisierungen bauen auf dem Grundprinzip der informationellen Selbstbestimmung der Dateninhaber auf. Dateninhaber sind zunächst die Personen, deren Daten gespeichert und verarbeitet werden. Zu den personenbezogenen Daten gehören Name, Geschlecht, Familienstand, Anschrift, Telefon, E-Mail und Bankverbindung. Ebenso dazu gehören biometrische Daten wie Fingerabdruck oder Iris-Scan sowie genetische Daten (DNS). Niemand muss dulden, dass gegen seinen Willen seine Daten erhoben, gespeichert, verarbeitet oder verkauft werden. Das bedeutet für die Datenverarbeitung folgende Grundsätze:

1. **Verbot mit Erlaubnisvorbehalt**
2. **Zweckbindung**
3. **Transparenz**
4. **Datenminimierung**
5. **Richtigkeit**
6. **Datensicherheit**

Nachfolgend gehen wir kurz auf diese Grundsätze ein.

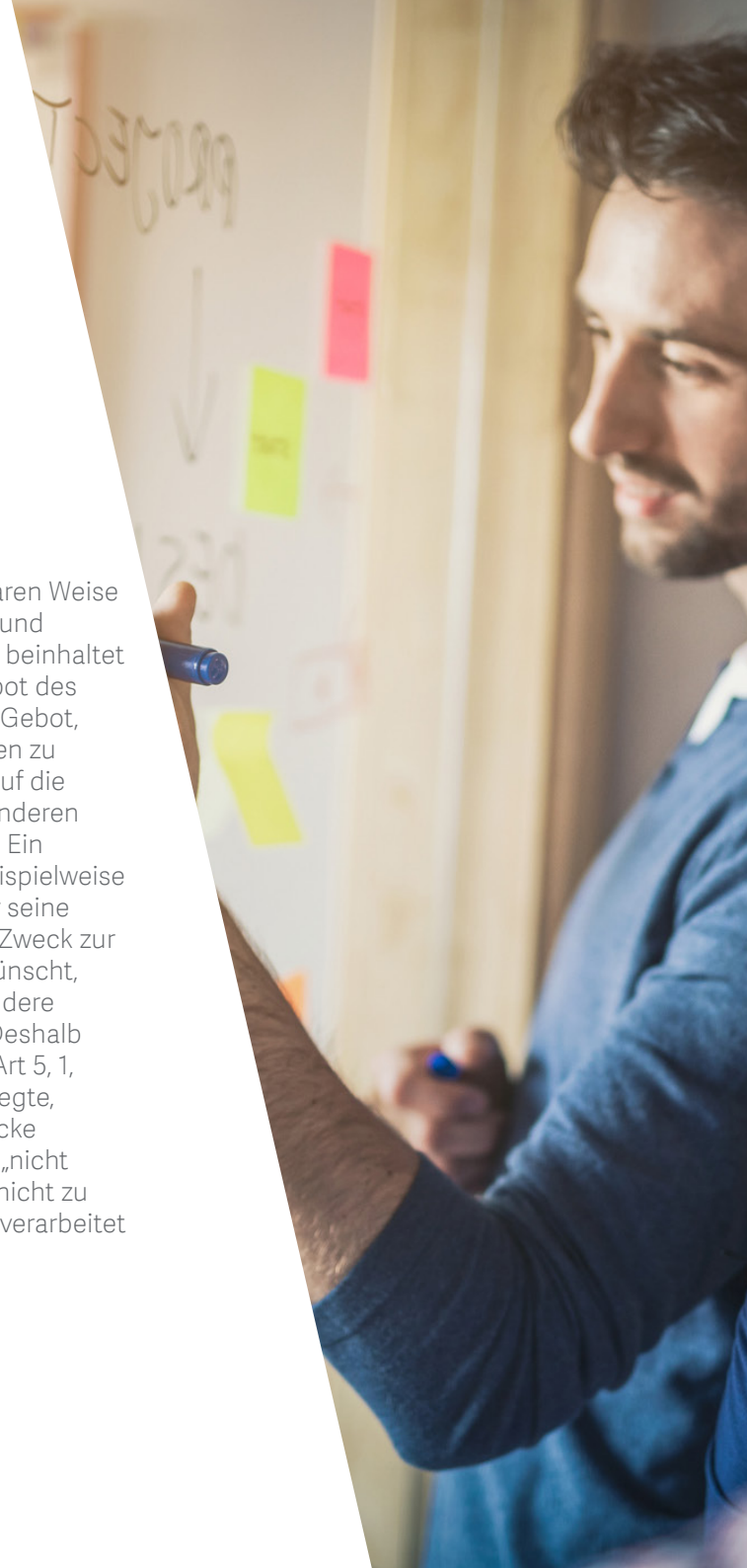
2.1 Verbot mit Erlaubnisvorbehalt (Zustimmung)

In Art. 6 der EU-DSGVO ist bestimmt, dass die Verarbeitung von personenbezogenen Daten grundsätzlich verboten ist, es sei denn, dass der Dateninhaber der Verarbeitung zustimmt.

2.2 Zweckbindung, Transparenz, Datenminimierung, Richtigkeit

Diese Anforderungen sind in Art 5 EU-DSGVO formuliert. Dieser Artikel bedarf sicherlich einer Auslegung durch die Gerichte, so unbestimmt sind die dort verwendeten Begriffe. Gleichwohl ist es wichtig zum Verständnis der späteren Bestimmungen, wenn wir sie hier zumindest kurz skizzieren.

Daten sind in einer für den Dateninhaber nachvollziehbaren Weise (Transparenz) und nach Treu und Glauben zu verarbeiten. Dies beinhaltet beispielsweise auch das Verbot des Rechtsmissbrauchs und das Gebot, nicht nur vertragliche Pflichten zu erfüllen, sondern Rücksicht auf die Rechte und Interessen des anderen Vertragspartners zu nehmen. Ein solches Interesse besteht beispielweise darin, dass der Dateninhaber seine Daten für einen bestimmten Zweck zur Verfügung stellt und nicht wünscht, dass seine Daten auch für andere Zwecke eingesetzt werden. Deshalb steht zur Konkretisierung in Art 5, 1, b, dass Daten nur „für festgelegte, eindeutige und legitime Zwecke erhoben werden“ dürfen und „nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.“



Daraus folgt dann auch die Maßgabe der Datenminimierung. Gemeint ist damit, dass die Datenverarbeitung dem Zweck angemessen sowie auf das „für die Zwecke der Verarbeitung notwendige Maß beschränkt sein" muss. Die Maßgabe der Richtigkeit beinhaltet, dass die einmal erhobenen Daten „sachlich richtig und erforderlichenfalls auf dem neuesten Stand" sein müssen. Die datenverarbeitende Stelle muss „dabei [...] alle angemessenen Maßnahmen treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden".

2.3 Datensicherheit

Datensicherheit ist neben der Zulässigkeit der Datenerhebung und Verarbeitung im Zeitalter der Digitalisierung ein hohes Gut, das entlang einer schnellen technischen Entwicklung einem stetigen Wandel unterliegt. Die Gesetzgeber macht aus der Not eine Tugend und gibt daher lediglich Hinweise, wie die Sicherheit zu gewährleisten ist. Daten dürfen nach Art 5, Nr. 1, f nur „in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen."

2.4 Sicherheit der Verarbeitung nach Art 32 EU-DSGVO

Art 32 beschreibt zahlreiche Auflagen und Konsequenzen für die Datenerhebung, -speicherung und -verarbeitung. Er hat eine enorme Tragweite, der sich viele Unternehmen nicht immer bewusst sind. Mit Art 32 EU-DSGVO wird aber deutlich, dass Datensicherheit eine Sisyphos-Aufgabe ist, die niemals endet, solange Ihr Unternehmen auch nur einen Datensatz auf einem Rechner speichert. Es lohnt sich die Lektüre des Gesetzestextes in Auszügen, weil alle Maßnahmen zum Datenschutz darin beschrieben aber nicht final geregelt sind:

1. „Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten**; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung** der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

2. Bei der **Beurteilung des angemessenen Schutzniveaus** sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

4. Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese **nur auf Anweisung des Verantwortlichen verarbeiten**, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet."

2.5 Privacy bei Design und Privacy by Default

In der Konsequenz besagen Art 5 und Art 32 der EU-DSGVO, dass Sie eine Datenschutzorganisation über den gesamten Lebenszyklus personenbezogener Daten etablieren müssen. Dazu gehören technische und organisatorische Maßnahmen entlang der aktuell verfügbaren technischen Möglichkeiten, um eine Datenschutzverletzung erst gar nicht zu ermöglichen. Von der Konzeption bis zur Überwachung sind also alle Prozesse unter Maßgabe der Gesetze jeweils „State of the Art" zu gestalten. Experten bezeichnen diesen Grundsatz als „Privacy by Design". Dazu gehört als zweiter Grundsatz die Datensparsamkeit, auch als „Privacy by Default" bezeichnet. Datensparsamkeit meint eine Minimierung der Daten auf das Notwendige für den jeweiligen Zweck, eine Beschränkung des zugriffsberechtigen Personenkreise und letztlich die Pseudonymisierung und Verschlüsselung der Daten, wo immer dies möglich ist. Letzteres ist vor allem wichtig, wenn Sie Daten beispielsweise von datenverarbeitenden Dienstanbietern oder in der Cloud verarbeiten lassen. Auch diese müssen EU-DSGVO-konforme Prozesse nachweisen und sollten darüber ein Zertifikat von einer unabhängigen Prüforganisation vorlegen können.

Beides bedarf einer kontinuierlichen Überprüfung und Aktualisierung.

Kapitel 3

Betroffenenrechte und die Folgen für Unternehmen

Schon bisher räumten die Datenschutzgesetze der EU und der BRD den Dateninhabern umfangreiche Rechte an ihren Daten ein. Darüber hinaus verpflichteten die Gesetze Unternehmen, welche Informationen sie rund um die Datenverarbeitung unaufgefordert mitteilen mussten. Bisher konnten sich Unternehmen dieser Verpflichtung mit einer langatmigen Datenschutzerklärung entledigen, die die wenigsten Verbraucher lasen. Es reichte, diese per Checkbox zur Kenntnisnahme zu bestätigen.

Die EU-DSGVO erweitert in Art. 13 diese Auskunftspflichten erheblich und erteilt den Dateninhabern zusätzliche Rechte, über die sie unaufgefordert zu unterrichten sind.

Insbesondere müssen Sie jede Person darüber informieren:

- dass sie sich bei Aufsichtsbehörden wie dem Bundes- oder Landesdatenschutzbeauftragten beschweren können
- dass sie ihre Zustimmung zur Verarbeitung ihrer personenbezogenen Daten jederzeit widerrufen können
- sie Zugriff auf ihre personenbezogenen Daten und deren Korrektur oder Löschung haben also das „Recht auf Vergessen werden" haben
- wenn Sie Daten an Drittparteien weiterleiten. Auch diese haben auf Verlangen die Daten zu korrigieren oder zu löschen
- wenn Sie eine automatisierte Verarbeitung personenbezogener Daten und Profilierung vornehmen
- dass sie bestimmten Arten der Verarbeitung einzeln widersprechen können, beispielsweise Direktmarketing, einer automatisierten Verarbeitung oder der Profilierung.

Darüber hinaus muss ein Datenverarbeiter die Dateninhaber informieren, wie lange persönliche Daten gespeichert werden und den bestellten Datenschutzbeauftragten benennen. Neu ist auch, dass beispielsweise Kunden einen Dienstleister wie ihre Bank oder den Stromlieferanten wechseln dürfen und dabei ihre Daten mitnehmen können. Zudem haben Dateninhaber das Recht, gemeinnützige Organisationen zu mandatieren, ihre Rechte außergerichtlich oder vor Gerichten wahrzunehmen und Ansprüche in ihrem Namen geltend zu machen. Für das deutsche Zivilrecht ist diese Form der Sammelklage ein Novum.

Schriftliche Informationen erteilen und quittieren lassen

Diese Informationen müssen Sie dem Kunden schriftlich mitteilen und die Kenntnisnahme quittieren lassen. Online erfolgt dies durch eine Checkbox, die der Kunde anklicken muss. Bei schriftlichen Verträgen erfolgt die Einbindung der Datenschutzinformationen durch eine Unterschrift.

Kapitel 4
Was Unternehmen jetzt tun sollten

Von der EU-DSGVO und dem nationalen Recht nach BDSG sind also praktisch alle Unternehmen betroffen, die innerhalb der EU personenbezogene Daten von Kunden, Lieferanten oder anderen Personen in ihrem Umfeld erheben, speichern und verarbeiten. Auch Unternehmen, die ihren Hauptsitz außerhalb der EU haben, innerhalb der Gemeinschaft aber Waren oder Dienstleistungen vertreiben, unterstehen ebenfalls der EU-DSGVO.

Um Ihr Unternehmen auf die EU-DSGVO vorzubereiten, sollten Sie folgende Maßnahmen ergreifen

1. Analyse aller bisherigen Verfahren und Prozesse der Datenverarbeitung und Anpassung derselben gemäß EU-DSGVO und BDSG in allen datenverarbeitenden Abteilungen

   a. Technisch
   b. Organisatorisch
   c. Personell

2. Dokumentation ihrer Datenschutzmaßnahmen und Einführung von Risk Assessment und Privacy Impact Assessment
3. Neufassung der Datenschutzerklärung sowie der Einwilligungserklärungen
4. Neue Prozesse definieren …

   a. wie mit dem Widerruf einer Einwilligung verfahren wird
   b. wie bei Korrekturen und Löschbegehren reagiert wird
   c. wie bei einer Datenschutzverletzung zu reagieren ist

5. Überprüfung und Ergänzung aller Verträge

   a. Auftragsdatenverarbeitung
   b. Allgemeine Geschäftsbedingungen
   c. Betriebsvereinbarungen
   d. Arbeitsverträge

6. Entwicklung und Durchführung von Mitarbeiterschulungen.

Nachfolgend skizzieren wir grob den Umfang der nun anstehenden Aufgaben für Geschäftsführer, Verantwortliche für Human Resources sowie Finanz- und Rechnungswesen.

4.1 Aufgaben für die Geschäftsleitung

Für die Umsetzung der EU-DS-GVO ist in vielen Unternehmen jemand in der IT verantwortlich und je nach Art und Größe des Unternehmens vielleicht auch ein Datenschutzbeauftragter zuständig. Und weil die EU-DSGVO etwas unbequem ist und nur wenige wissen, wie sie umzusetzen ist, wird die Verantwortlichkeit gerne wie ein Schwarzer Peter herumgereicht. Aber Sie als Geschäftsführer halten immer den Kopf hin, wenn es zu einer Datenschutzverletzung kommen sollte. Es ist daher ratsam, dass Sie die notwendigen Maßnahmen zur Anwendung der EU-DSGVO in Ihrem Unternehmen steuern und vor allem die Umsetzung überwachen.

4.2 Team zur Umsetzung der EU-DSGVO zusammenstellen

Stellen Sie zunächst ein Team zusammen mit Führungskräften aus den Abteilungen IT, Personal, Marketing / Vertrieb sowie dem Finanz- und Rechnungswesen. Erstellen Sie einen Fahrplan für Ihr Unternehmen, wie Sie die EU-DSGVO umsetzen wollen. Verteilen Sie die Aufgaben, die nun anstehen. Lassen Sie eine Dokumentation Ihrer Datenschutzmaßnahmen erstellen und welche technischen und organisatorischen Maßnahmen Ihr Unternehmen ergriffen hat.

Nutzen Sie für Ihren Fahrplan und die Umsetzung unsere **Checkliste: EU-DSGVO für Geschäftsleiter**.

4.3 Aufgaben für die HR-Abteilung

Die Personalabteilung arbeitet täglich mit einer Unmenge an persönlichen und personenbezogenen Daten. Viele HR-Manager nutzen die automatisierten Prozesse der großen Stellenbörsen im Internet. Sie setzen im besten Falle BDSG-konforme HR-Management-Systeme ein und nutzen für die Entgeltabrechnung zusammen mit der Buchhaltung, Systeme aus der Cloud, wie die von Sage. Vorteil bei der Datenverarbeitung in der Cloud ist, dass nur wenige Konzerne eine IT-Sicherheit realisieren können, wie dies Cloud-Anbieter praktizieren. Und nur nebenbei sei angemerkt, dass die deutsche Sage GmbH als Auftrags-Datenverarbeiter mit seinem großen Rechenzentrum in Frankfurt am Main die EU-DSGVO zum Stichtag 25. Mai 2018 selbstverständlich zu 100 Prozent erfüllt. Das aber bewahrt Ihr Unternehmen nicht vor möglichen Datenschutzverletzungen. Ebenso wenig können Sie Ihre Datenschutzaufgaben einfach an die IT delegieren. Bestenfalls macht Sie Ihr CIO oder der IT-Leiter darauf aufmerksam, dass Sie Ihre Mitarbeiter zum sorgfältigen Umgang mit den Daten der Kollegen und Bewerber anhalten sollen. Dafür aber müssen Sie als HR-Chef vor allem Ihre internen Prozesse EU-DSGVO-konform gestalten.

4.4 Prozesse für Daten-Zugang und Zugriff mit Rollen und Rechten definieren

In einer HR-Abteilung herrscht ein ständiges Kommen und Gehen. Da werden Krankmeldungen abgegeben, Bescheinigungen abgeholt; Fest- und Teilzeitangestellte, Zeitarbeitskräfte, Trainees, Praktikanten und Aushilfen und manchmal sogar deren Angehörige regeln mit den HR-Mitarbeitenden wichtige Angelegenheiten. Bewerber warten auf ihre Gespräche, Mitarbeiter auf ihre Papiere. Und selbst wenn Sie bereits alle Prozesse elektronisch abbilden und eigentlich ein papierloses HR-System etabliert haben: Irgendwas will irgendwer dennoch lieber persönlich klären. Parallel finden immer auch Datenverarbeitungsprozesse statt. Dann strahlen auf Monitoren personenbezogene Daten, während die Sachbearbeiter in ein Gespräch vertieft oder gerade aus dem Zimmer sind, um eine persönliche Angelegenheit zu erledigen. Schnell huscht mal ein Unbefugter in ein Büro und macht mit seinem Smartphone einen Screenshot. Aber es geht noch schlimmer: Schnell ist ein kompletter Datensatz auf ein USB-Stick gezogen, ein Druckbefehl an einen entfernten Drucker gesendet. Ruck-Zuck in wenigen Sekunden sind hunderte Daten gestohlen, ohne dass es auch nur jemand geahnt hätte. Der Schutz vor dem Zugriff Unbefugter auf personenbezogene Daten in der HR-Abteilung kann gar nicht hoch genug sein. Eine EU-DSVGO-konforme HR-Abteilung muss daher schon baulich bestimmte Anforderungen erfüllen und zusätzlich elektronische Barrieren errichten, um einen Datenklau unmöglich zu machen. Des Weiteren müssen alle datenverarbeitenden Mitarbeiter für den Umgang mit diesen Daten gesonderte Verschwiegenheitserklärungen unterschreiben, in der sie auch die Kenntnisnahme ihrer besonderen Obliegenheiten bestätigen.

Welche Schutzmaßnahmen Sie und Ihr Unternehmen in der Personalabteilung vor dem 25. Mai 2018 einführen sollten, lesen Sie in unserem **Leitfaden: Die EU-DSGVO für die HR-Abteilung.**

4.5 Aufgaben für Buchhaltung und Rechnungswesen

Wie die Personalabteilung geht auch die Buchhaltung sowie das Finanz- und Rechnungswesen jeden Tag mit personenbezogenen Daten um. Die Empfehlungen zu Daten-Zugang und Zugriff mit Rollen und Rechten sowie unsere **Checkliste 2: EU-DSGVO für die HR-Abteilung** gelten daher uneingeschränkt auch für das Rechnungswesen. Überhaupt war ja die Buchhaltung immer schon Pionier beim Einsatz von Software und der Nutzung von Cloud-Diensten. Und weil sie dabei sehr oft auch für die Kundenstammdatenpflege zuständig waren, sollten bestimmte Anforderungen der EU-DSGVO auch in der Buchhaltung verortet werden. Hierbei ist es wichtig, neue Prozesse für die Pflege der Stammdaten aufzusetzen und die Auswahl sowie die Vertragsgestaltung mit Auftrags-Datenverarbeitern in der Cloud zu überprüfen.

Welche Schutzmaßnahmen Sie in Ihrer Buchhaltung vor dem 25. Mai 2018 einführen sollten, lesen Sie in unserem **Leitfaden: Die EU-DSGVO für die Buchhaltung.**

4.6 Auftragsdatenverarbeitung in der Cloud

Grundsätzlich gilt für die Auftragsdatenverarbeitung in der Cloud, dass sie innerhalb der EU und damit in der örtlichen Zuständigkeit der EU-DSGVO zulässig ist. Das gilt auch für Steuer- und Buchhaltungsdaten. Der Cloud-Nutzer als verantwortliche Stelle und der Cloud-Provider müssen aber geeignete Maßnahmen zum EU-DSGVO-konformen Datenschutz nachweisen. Neu ist zudem in der EU-DSGVO, dass auch der Cloud-Anbieter als Auftrags-Datenverarbeiter für Datenschutzverletzungen haftbar gemacht werden kann, wenn er sich Fehler zurechnen lassen muss. Die Übermittlung von personenbezogenen Daten in ein Drittland außerhalb der EU ist ebenfalls möglich, wenn der Cloud-Anbieter ein EU-DSGVO-konformes Schutzniveau nachweist und dafür auch Garantien abgibt, dass „geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet". Diesen Nachweis kann er durch eine Zertifizierung nach der EU-DSGVO nachweisen. Zudem muss die EU-Kommission dieses Zertifikat anerkannt haben.

4.7 Der Brexit und die Folgen für Unternehmen in Europa

Nach dem Referendum in England zum EU-Austritt wird das Vereinigte Königreich voraussichtlich im März 2019 die Gemeinschaft verlassen. Bis zu diesem Datum gilt die EU-DSGVO uneingeschränkt auch in England weiter. Die englische Königin hat mit ihrer Rede im Juni 2017 zudem deutlich gemacht, dass England auch danach die Datenschutzregeln der EU beachten wird. Experten gehen daher davon aus, dass die Europäische Kommission England als ein Land einstuft, das einen angemessenen Datenschutz garantiert. Mit den entsprechenden Zertifikaten und der Anerkennung der EU-Kommission können britische Cloud-Anbieter also weiterhin in der EU ihre Dienstleistungen erbringen.

Über Sage

Sage ist Marktführer für integrierte Buchhaltungs-, Lohnabrechnungs- und Bezahlsysteme und unterstützt die Ambitionen von Unternehmern weltweit. Vor 30 Jahren begann Sage in Großbritannien selbst als ein kleines Unternehmen.

Heute unterstützen 13.000 Mitarbeiter in 23 Ländern Millionen Unternehmen dabei, die Weltwirtschaft anzutreiben.

Sage erfindet die Unternehmensführung neu und vereinfacht sie mit smarter Technologie. Dafür arbeitet Sage eng zusammen mit einer wachsenden Gemeinschaft von Gründern, Unternehmern, Steuerberatern, Partnern und Entwicklern. Als FTSE 100 Company ist sich Sage seiner gesellschaftlichen Verantwortung bewusst. Das Unternehmen hilft an seinen Standorten ortsansässigen Verbänden und Hilfebedürftigen durch die hauseigene Stiftung, die Sage Foundation.

Im deutschen Mittelstand ist die Sage GmbH mit 250.000 Kunden und mehr als 1.000 Fachhändlern einer der Marktführer für betriebswirtschaftliche Software und Services.

Im Geschäftsjahr 2014/2015 erwirtschaftete Sage in Deutschland einen Umsatz von über 100 Millionen Euro und beschäftigte ca. 800 Mitarbeiter, die eines genau im Blick haben: den Erfolg und das Wachstum Ihres Unternehmens.

Rechtshinweis

Sage GmbH

Franklinstraße 61-63
D-60486 Frankfurt am Main

Telefon: 069 50007-6300
E-Mail: info@sage.de
www.sage.com