Whitepaper

EU-Datenschutz-grundverordnung

Grundlegende Neuerungen,
Begriffe im Datenschutz,
Checklisten, und Vorgehensmodelle

Sage

Vowort und Inhalt

Die DSGVO ist ein komplexes Thema, das nicht nebenbei zu managen ist. Der Blick in österreichische und europäische Unternehmen zeigt, dass Informations- und Handlungsbedarf besteht.

Dieses Whitepaper will mit Informationen und Guidelines beitragen, damit Sie die in Ihrem Unternehmen erforderlichen Maßnahmen bis zum Stichtag 25. Mai 2018 umsetzen können. Sie finden darin Erklärungen grundlegender Neuerungen und Begriffe im Datenschutz, Checklisten, sowie Vorgehensmodelle.

Was ist die DSGVO und wer ist davon betroffen?

Praktisch jedes Unternehmen fällt seit dem 25. Mai 2018 unter die neue DSGVO, ergänzt durch das österreichische Datenschutz-Anpassungsgesetz, und die Strafen bei Versäumnis sind hoch. Auf der anderen Seite besteht die Chance, die Verarbeitung von personenbezogenen Daten auf eine solide, bereinigte Basis zu stellen und mit einer verbesserten Data Governance auch das Vertrauen der Kunden zu steigern.

Die EU-Datenschutzgrundverordnung (DSGVO) wurde vom europäischen Parlament beschlossen und trat am 25. Mai 2018 in Kraft. Mit dieser Verordnung wurden nationale Datenschutzgesetze vereinheitlicht, Unternehmen in allen EU-Staaten müssen dieselben Regeln anwenden. Ebenso gelten diese für weltweite Firmen, die ihre Leistungen innerhalb der EU anbieten - sowohl vor Ort, als auch online. Wer bis zum Stichtag seine Datenanwendungen nicht angepasst hat, dem drohen hohe Strafen, nämlich bis 20 Mio. Euro oder bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes.

Die Konsumenten bekommen mit der DSGVO mehr Rechte zu wissen und zu entscheiden, was mit ihren persönlichen Daten passiert, die sie an Unternehmen weitergeben. Ihre Daten dürfen nur nach Zustimmung gespeichert werden und Unternehmen müssen jederzeit Auskunft geben können, welche Daten sie besitzen. Die Verordnung betrifft neben Kundendaten auch jene von Mitarbeitern, Lieferanten und Partnern. Jede Organisation, die personenbezogene Daten von natürlichen Personen, die sich in der EU befinden, verarbeitet oder speichert, ist demnach von der Verordnung betroffen – das ist praktisch jedes Unternehmen.

Oft wird im Zuge der Diskussion um die DSGVO nicht bedacht, dass es auch weiterhin ein österreichisches Datenschutzgesetz gibt. Die Regelungen des DSG2000 wurden ebenfalls am 25. Mai 2018 durch das Datenschutz-Anpassungsgesetz ersetzt, welches gleichzeitig mit der DSGVO anzuwenden ist. Der Nationalrat hat darin etwa Präzisierungen zum Datenschutzbeauftragten oder Regeln zum Datengeheimnis und zur Datenverarbeitung zu spezifischen Zwecken beschlossen.

Künftig wird es keine Meldepflicht mehr bei der Datenschutzbehörde (Datenverarbeitungsregister) geben, dafür haben sowohl die Verantwortlichen (Auftraggeber) als auch die Auftragsverarbeiter (Dienstleister) weitreichend neue Pflichten bei der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten. Für Unternehmen geht es darum, zu erfassen, wo personenbezogene Daten gespeichert sind, zu beachten sind u.a. Mehrfachablagen. Augenmerk gilt genauso unstrukturierten Daten, die ebenfalls Rückschlüsse auf Personen zulassen können. Die DSGVO betrifft auch Unternehmen, die ihre Daten bei einem Cloud-Anbieter speichern oder die Services, wie etwa die Lohnverrechnung, outgesourct haben.

Bedarf an Aufklärung und Informationen

Verschiedene Umfragen lassen aufhorchen, denn in relativ vielen Unternehmen herrscht weiterhin Unklarheit über Anforderungen, Umsetzung und Konsequenzen der DSGVO. Jene, die sich aber damit bereits befasst haben, sehen durchaus die Vorteile der neuen Regelungen.

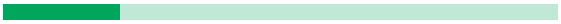
Immerhin 75 Prozent der österreichischen Unternehmen haben sich bereits grundsätzlich mit den Anforderungen der DSGVO auseinandergesetzt. Nur 21 Prozent sind sich jedoch bewusst, dass als Strafe bis zu 4 Prozent des weltweiten Jahresumsatzes fällig werden können.

Unklarheit besteht darüber, welche personenbezogenen Daten (pbD) geschützt werden müssen:

50 % wissen nicht, dass das Geburtsdatum geschützt werden muss

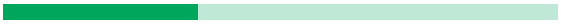
37 % meinen, ihre Marketing Datenbank enthält keine pbD

29 % stufen Adressen von Kunden nicht als pbD ein



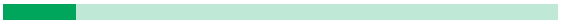
21 % glauben, E-Mail Adressen seien keine pbD

Zusätzlich wissen viele nicht, wer für die Umsetzung der DSGVO zuständig ist. Wer ist aus Unternehmenssicht verantwortlich?



35 % CEO

67 % IT-Abteilung

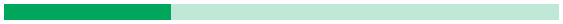


13 % CISO – Chief Information Security Officer

Quelle: Computerwelt / Trend Micro Studie September 2017, http://www.computerwelt.at/news/technologie-strategie/security/detail/artikel/122029-viele-unternehmen-sind-noch-nicht-auf-umsetzung-der-eu-datenschutzgrundverordnung-vorbereit/

Eine Studie mit internationalen Führungskräften zeigt: 45 Prozent haben einen strukturierten Prozess um sich DSGVO-fit zu machen, davon sind jedoch nur 66 Prozent sicher, dass dieser auch zum Erfolg führen wird. Erwartete Vorteile:

71 % Verbesserung der Data Governance



30 % Image-Aufwertung

29 % steigende Kundenzufriedenheit

Quelle: SAS Studie Oktober 2017, www.sas.com/de_at/news/press-releases/2017/oktober/sas-studie-zur-datenschutz-grundverordnung--dsgvo-wird-zur-zerre.html

DSGVO im HR-Bereich

Gerade für die sensiblen Daten von HR spielt die DSGVO eine wichtige Rolle, aber 44 % der befragten 1.800 Personaler und Lohnbuchhalter aus 9 europäischen Ländern haben keine Ahnung, worum es sich bei der DSGVO handelt. Von den 56 % welche die DSGVO kennen, sind allerdings 71 % überzeugt, dass die Datensicherheit künftig höher ist und 81 % meinen, die Anforderungen rechtzeitig zu erfüllen. Dagegen sind aus Österreich nur zwei Drittel der Meinung, dass ihre Personalmitarbeiter die Anforderungen der DSGVO bis zum Ablauf der Frist vollumfänglich erfüllen werden.

Quelle: SD Worx Studie HR November 2017, www.sdworx.de/de-de/presse/2017-11-28-hr-manager-ignorieren-dsgvo

Die wesentlichen Neuerungen und Begriffe

Dateninhaber: personenbezogene Daten, Verbot mit Erlaubnisvorbehalt
Die DSGVO verstärkt die Rechte von Einzelpersonen – sie sind die Dateninhaber – und legt fest, welche Informationen sie über die Verarbeitung ihrer Daten erhalten müssen. Dies betrifft die personenbezogenen Daten, dazu gehören Name, Adresse, Telefon, E-Mail, Bankverbindung, Sozialversicherungsnummer, Geschlecht, Familienstand und auch biometrische Daten wie Fingerabdrücke – also sämtliche Informationen, die eine Person identifizierbar machen. Die Datenverarbeitung muss sicherstellen, dass gegen den Willen der Dateninhaber keine ihre Daten erhoben, gespeichert, verarbeitet oder weitergegeben bzw. verkauft werden. Das bedeutet gemäß dem Verbot mit Erlaubnisvorbehalt: Prinzipiell ist die Verarbeitung personenbezogener Daten verboten, Unternehmen müssen die Zustimmung der Dateninhaber durch eine Erklärung einholen.

Die Einwilligung ist unter bestimmen Voraussetzungen nicht notwendig, wie z. B. wenn, die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, welcher der Verantwortliche unterliegt (Artikel 28 1/c).

Privatsphäre: Privacy by Design und Privacy by Default
Solange personenbezogene Daten in Ihrem Unternehmen gespeichert werden, also über den ganzen Lebenszyklus von erstmaliger Eingabe bis zur Löschung, muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass keine Datenschutzverletzung passieren kann – das wird mit Privacy by Design gewährleistet. Es ist jeweils der aktuelle Stand der Technik zu berücksichtigen. Technische und organisatorische Maßnahmen müssen regelmäßig geprüft und evaluiert werden. Anwendungen oder Auswahlfelder, müssen von Anfang an so eingestellt sein, dass sie größtmöglichen Datenschutz gewährleisten. Privacy by Default wird auch als Datensparsamkeit bezeichnet. Nur die für den jeweiligen Zweck erforderlichen Daten sollen verarbeitet werden, der Zugriff soll nur jenen Mitarbeitern möglich sein, die damit zu tun haben. Falls Ihre erfassten personenbezogenen Daten von Dritten verarbeitet oder gespeichert werden (Cloud-Dienstleistern), müssen Auftragsverarbeiter in einer Dienstleistervereinbarung die Konformität ihrer Prozesse nach der DSGVO nachweisen, ggf. ergänzt durch ein Zertifikat einer unabhängigen Prüf-Organisation.

Betroffenen-Rechte
Wenn Sie Daten einer Person speichern oder verarbeiten, müssen Sie diese Person über eine Reihe von Punkten schriftlich informieren und das auch bestätigen lassen, durch eine Unterschrift oder online mittels Anklicken einer Checkbox. Das betrifft u.a. folgende Punkte:

- Die **Zustimmung** zur Verarbeitung personenbezogener Daten kann jederzeit **widerrufen** werden. Jede Person kann auch einzeln bestimmten Verarbeitungsarten widersprechen, etwa Direktmarketing oder Profiling.
- **Recht auf Vergessen werden:** Daten müssen auf Verlangen korrigiert oder gelöscht werden. Diese Pflicht betrifft auch Dritte, an welche die Daten eventuell weitergeleitet wurden.
- Recht auf Datenübertragbarkeit: Auf Antrag der Person müssen ihr alle Daten in einem lesbaren gängigen Format zur Verfügung gestellt werden. So können Kunden auch bei Wechsel eines Dienstleisters, wie einem Stromlieferanten, ihre Daten zur Konkurrenz mitnehmen.
- **Recht auf Auskunft:** Umfasst u. a. welche und wie lange Daten gespeichert werden oder die Logik bei automatisierter Verarbeitung.

Neu ist auch, dass Betroffene gemeinnützige Organisationen beauftragen können, im Rahmen einer **Sammelklage** ihre Rechte zu vertreten. Das war bis jetzt nicht möglich, betrachtet man die Initiativen des österreichischen Datenschutz-Aktivisten und Juristen Max Schrems.

Verzeichnis von Verarbeitungstätigkeiten
Die Beweispflicht, dass die DSGVO eingehalten wird, muss das Unternehmen erbringen. Dazu benötigt es entsprechende Systeme, welche die korrekte Speicherung und Verarbeitung der personenbezogenen Daten nachweisen können, das **Verzeichnis von Verarbeitungstätigkeiten**.

Weitere Verpflichtungen betreffen das Benennen eines **Datenschutz-Beauftragten**, sowie die Meldung an die Aufsichtsbehörde und an betroffene Personen **im Falle eines „data breach“**; etwa eines Hacker-Angriffs oder des Verlusts eines Datenträgers, wenn dadurch Unbefugte Zugriff auf personenbezogene Daten erhalten.

Wie Sie sich auf die DSGVO vorbereiten

Die Vorbereitung und Umsetzung der Maßnahmen betrifft das gesamte Unternehmen und ist nur im Team durchführbar, bestehend aus Geschäftsführung, Vertrieb, Marketing, Finanz, Personal und IT.

Erstellen einer Maßnahmen–Checkliste mit Zeitplan und Verantwortlichen

- **Ist-Analyse:** Auflistung aller Prozesse und damit verbundenen Anwendungen, welche personenbezogene Daten verarbeiten.
- **Soll-Zustand:** Analyse der technischen, organisatorischen und personellen Maßnahmen, welche sind im Sinne der DSGVO und des Datenschutz-Anpassungsgesetzes erforderlich sind.
- **Verzeichnis**, wo wie und zu welchem Zweck Daten verarbeitet werden.
- **Dokumentation aller Datenschutzmaßnahmen** und wie wird Privacy by Design und Privacy by Default umgesetzt.
- **Datenschutzfolgenabschätzung** (Risk und Privacy Impact Assessment)
- Sicherstellung der Einhaltung der **Betroffenen-Rechte**
  - Anpassen von Datenschutz- und Einwilligungs-Erklärungen
  - Verfahren bei Widerruf der Zustimmung
  - Verfahren bei Antrag auf Korrekturen oder Löschen (Recht auf Vergessen)
  - Verfahren bei Antrag auf Datenübertragung
  - Auskunft über gesammelte Daten geben
- Neuen **Prozess** definieren für den Fall einer Datenschutzverletzung
- Ernennen eines Datenschutz-Beauftragten (wenn erforderlich)
- Anpassen aller betroffenen **Verträge**
- **Schulen** der MitarbeiterInnen

Zusätzliche Maßnahmen, wenn Sie Cloud-Dienste nutzen

Wenn Sie Software as a Service (SaaS) nutzen, etwa Ihre Buchhaltung oder Lohnverrechnung ausgelagert haben, oder wenn Abteilungen Daten bei einem Cloud-Service Provider speichern, so ist dies innerhalb der EU zulässig, hier gilt ja für alle dieselbe DSGVO. Folgt man den aktuellen Stellungnahmen, so ist davon auszugehen, dass England auch nach dem Brexit die DSGVO berücksichtigen und demnach von der EU-Kommission anerkannt wird. Werden personenbezogenen Daten in ein Drittland außerhalb der EU exportiert, so muss dieser Cloud Provider ein DSGVO-konformes Datenschutzniveau nachweisen, etwa durch ein von der EU anerkanntes Zertifikat. Neu ist, dass auch der Cloud-Anbieter für Datenschutzverletzungen haftbar gemacht werden kann. Beide Seiten, also Cloud-Nutzer und -Anbieter, müssen jedenfalls alle Datenschutzmaßnahmen konform dokumentieren.

Dienstleister-Vereinbarungen müssen Sie daher überprüfen und ggf. anpassen.

Spezielle Hinweise und Checklisten für Geschäftsführer
Wenn es zu einer Datenschutzverletzung kommt, trägt letztendlich der Geschäftsführer die Verantwortung. Daher ist es seine vorrangige Aufgabe, die Maßnahmen zur Umsetzung der DSGVO zu steuern. Dazu gehören:

- Zusammenstellen eines **Teams** aus allen Abteilungen
- Festlegen eines **Fahrplans**, um den Soll-Zustand zu erreichen
- Zusätzliches Augenmerk auf **IT-Themen** wie Schutz des Rechenzentrums vor Elementarschäden, Zugriffsberechtigungen und Rollen, Passwort-Policy, Maßnahmen gegen Datenverlust (Sicherung und Backup), Einbeziehen aller mobilen Endgeräte
- Überwachen der **Umsetzung**
- **Schriftliche Dokumentation** der Datenverarbeitung inklusive wie die Anwendung der Sicherheitsmaßnahmen überwacht wird; die Dokumentation muss auf Verlangen der Behörde vorgelegt werden

Mit der Umsetzung des Soll-Zustandes ist es nicht getan. Im Zuge von technischen Weiterentwicklungen ist das erstellte Konzept regelmäßig zu prüfen und anzupassen.

Spezielle Hinweise und Checklisten für HR
Personalabteilungen arbeiten mit sensiblen Daten von Mitarbeitern und Bewerbern. Hier ist besondere Sorgfalt geboten, alle internen Prozesse entsprechend der DSGVO zu gestalten. Um personenbezogene Daten vor dem Zugriff Unbefugter zu schützen, muss HR auf folgendes zusätzlich achten:

- Zutrittskontrolle zu den Büros für Mitarbeiter plus zusätzliche Zugangskontrollen für Besucher, wie etwa Bewerber: Mit eigenen getrennten Räume verhindern Sie, dass Fremde einen Blick auf Bildschirme werfen und dort Daten ablesen können.
- Die Datensicherheit sei nochmals in wesentlichen Punkten wiederholt: Welche Mitarbeiter müssen welche sensiblen Daten sehen oder bearbeiten können; Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben wurden – daher auch nicht zweckfremd weitergegeben werden; Daten für unterschiedliche Zwecke daher trennen, etwa Personalakten von der Lohnverrechnung.
- Mitarbeiter, die personenbezogene Daten verarbeiten, müssen gesonderte **Verschwiegenheitserklärungen** unterschreiben.
- Daten müssen jederzeit auf Anfrage **zur Verfügung** gestellt werden können.
- **Daten von Bewerbern:** Diese Daten kommen aus Ihren eigenen Systemen oder von fremden Bewerbungs-Plattformen; wenn Sie die Einwilligung der Kandidaten zur Speicherung einholen, können Sie zugleich die Erlaubnis abfragen, die Daten auch länger in einem Bewerber-Pool speichern zu dürfen; ohne Einwilligung müssen Sie die Daten aller ausgeschiedenen Kandidaten wieder löschen.

Spezielle Hinweise und Checklisten für die Buchhaltung
Die Buchhaltung hat ebenfalls mit sensiblen Daten zu tun, speziell betrifft das die Eingabe und Wartung der Stammdaten von Kunden, Lieferanten und Partnern. Generell gelten ähnliche Sorgfaltsmaßnahmen wie bei HR, besonders ist zu beachten:

- Wenn ein **Dateninhaber** einwilligt, personenbezogene Daten zur Verfügung zu stellen, so ist er jedes Mal **auf seine Rechte hinzuweisen**.
- Schaffen Sie entsprechende **Links und Formulare für den Dateninhaber**, wo er seine Rechte ausüben kann (wie Berichtigung, Vergessen werden, Widerruf, Einschränkung der Verarbeitung).
- Sorgen Sie mit definierten **Prozessen für eine rasche Bearbeitung** des Vorgangs (der angemeldeten Rechte) innerhalb von 2 Arbeitstagen.

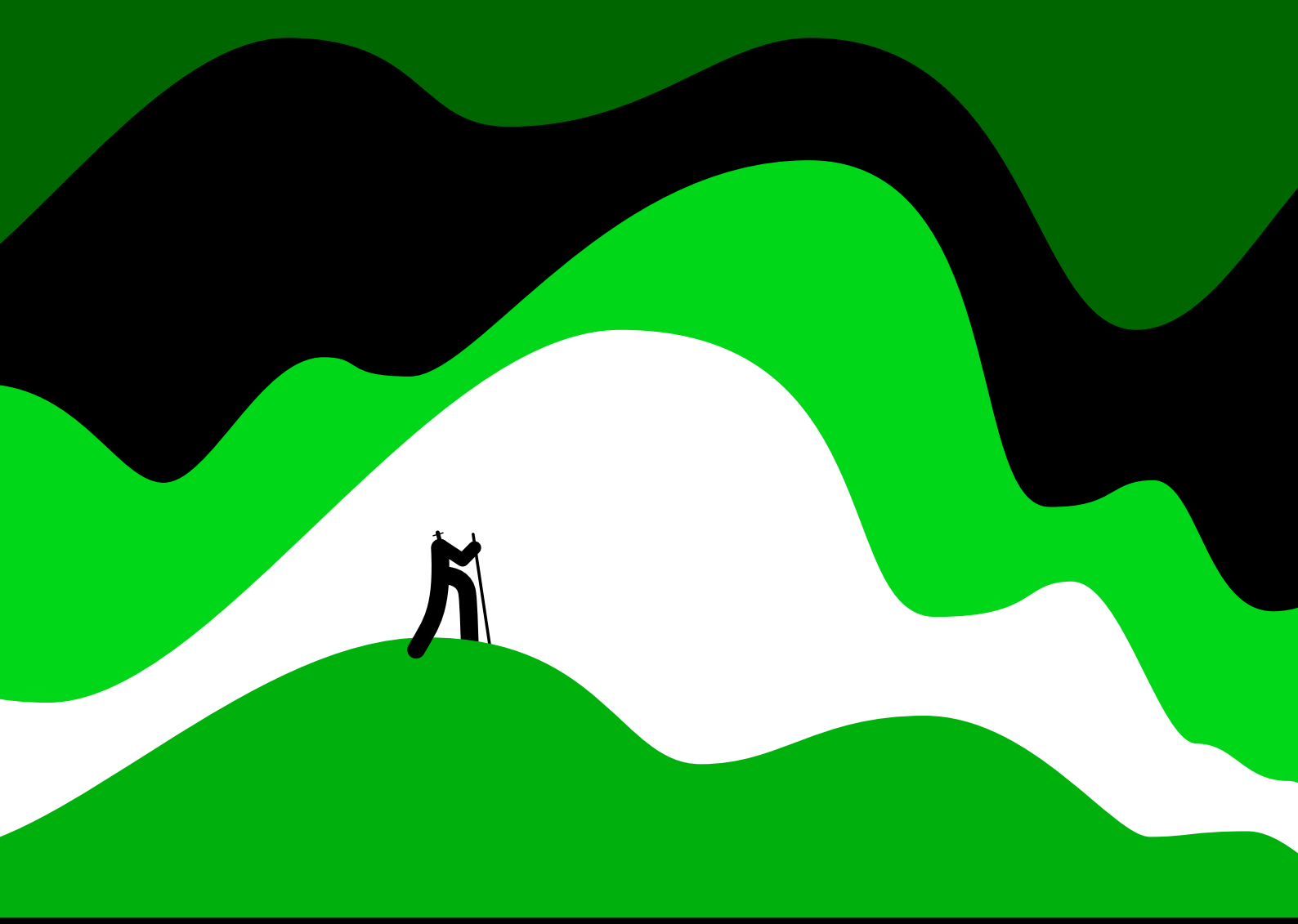
Checkliste für Fragen an Ihren Software-Partner

Sprechen Sie Ihren Software-Anbieter bzw. -Dienstleister auf die Änderungen im Zusammenhang mit der DSGVO an. Sage DPW ist übrigens bestens auf die DSGVO vorbereitet und erfüllt alle notwendigen Voraussetzungen. Wählen Sie die für Ihre Situation zutreffenden Fragen an Ihren Software-Partner:

- ☐ Arbeitet der Anbieter mit einem Consultant zusammen, der mit rechtlicher Beratung zur DSGVO unterstützt?
- ☐ Wird für Fernwartung ein zertifiziertes Programm (Viewer) genutzt, das sicherstellt, dass der Datenstrom nicht entschlüsselt werden kann (gegen sog. Man-in-the-middle-Attacken)?
- ☐ Kann das Rechenzentrum technische und organisatorische Maßnahmen nachweisen zum Schutz vor Katastrophen und Hacker-Angriffen?
- ☐ Gibt es vorab eine Risikofolgenabschätzung für Verarbeitungen, wo aufgrund neuer Technologien oder aufgrund von Art und Umfang ein Risiko für den Schutz personenbezogener Daten besteht?
- ☐ Gibt es Unterstützung beim einmaligen Löschen von sensiblen, nicht erforderlichen Daten in Form von Analyse, Test und Umsetzung mittels Löschprogramm sowie Dokumentation darüber?
- ☐ Gibt es pro Programm bzw. pro Modul ein Verfahrensverzeichnis, das alle Datenkategorien und die möglichen Empfänger in einer Liste anführt und welches dann – je nach Nutzung der Datenfelder – individuell angepasst werden kann?
- ☐ Betreffend das Recht auf Vergessen: Gibt es Funktionen zum vollständigen Löschen von Mitarbeitern oder Bewerbern mit allen zugehörigen Daten?
- ☐ Können Passwörter und Berechtigungen so genutzt und eingestellt werden, dass sie den neuen Anforderungen entsprechen?
- ☐ Gibt es einen gesicherten Prozess, dass der Dienstleister nach schriftlicher Anforderung die Daten der antragstellenden Person löscht?
- ☐ Kann jeder Mitarbeiter sehen, welche Daten von ihm gespeichert sind und wer/was/wann geändert oder gelöscht hat?
- ☐ Betreffend das Recht auf Auskunft: Gibt es eine Funktion, mit der sämtliche gespeicherte Daten einer Person in lesbarem Format, z. B. als PDF, dargestellt werden können?
- ☐ Gibt es für HR in der Bewerberverwaltung eine Funktion „Einwilligungserklärung für zeitlich unbegrenzte Datenspeicherung“? Wird das geplante Löschdatum automatisch gespeichert?

Fazit

Bei der Umsetzung der DSGVO sollte es in erster Linie nicht darum gehen, Strafen zu vermeiden. Vielmehr ist es die Chance, die Hoheit über die im Unternehmen gespeicherten Daten zu wahren oder in manchen Fällen vielleicht auch zurück zu gewinnen. Und im Grunde werden das Recht auf Privatsphäre und auf Vergessen wichtige Themen unseres digitalen Zeitalters. In diesem Sinne bedeuten zwar die im Rahmen der DSGVO umzusetzenden Maßnahmen einen Aufwand, sie werden jedoch das Image Ihres Unternehmens als vertrauenswerter Dienstleister stärken.



Sage GmbH

Stella-Klein-Löw-Weg 15
1020 Wien

+43 1 277 04
info@sagedpw.at

www.sagedpw.at

Sage GmbH ist mit der Sage DPW-Produktpalette führender Anbieter für Personalmanagement-Software. Mit unserem umfassenden Produktportfolio bieten wir Softwarelösungen für alle Bereiche des Personalwesens. Sage DPW-Software ist bei über 1.000 Kunden implementiert, vom mittelständischen bis zum multinationalen Unternehmen, in verschiedensten Branchen.