DIE EU-DATENSCHUTZ-GRUNDVERORDNUNG

Mit Print und Document Management den Datenschutz verbessern

IDC ANALYZE THE FUTURE

MÄRZ 2018
GESPONSERT VON TA TRIUMPH-ADLER

VERSCHLAFEN UNTERNEHMEN IN DEUTSCHLAND DIE DSGVO?

Der Datenschutz hat seit jeher einen hohen Stellenwert in Deutschland. Seit mehr als 40 Jahren gibt es strenge Datenschutzbestimmungen. Doch die Relevanz des Themas wird derzeit durch die EU-Datenschutz-Grundverordnung (DSGVO) noch einmal erhöht. Die DSGVO beinhaltet Vorschriften für die Verarbeitung von personenbezogenen Daten und ist für alle Unternehmen in Deutschland ab Mai 2018 rechtsverbindlich.

Es ist somit dringend erforderlich, dass Unternehmen sich spätestens jetzt intensiver mit der DSGVO beschäftigen. Nicht nur wegen hoher Strafzahlungen oder Imagerisiken für das eigene Unternehmen, die bei Verstößen im Raum stehen. Vielmehr sollten Firmen die Verordnung als Anlass und als Chance betrachten, Prozesse im Unternehmen zu verbessern, für mehr Transparenz zu sorgen und der Firma die Spielregeln der Digitalisierung beizubringen. Denn diese legt die neue Verordnung zweifelsohne fest.

Der Blick in die Unternehmen verrät allerdings: Die DSGVO wird in Deutschland auf die leichte Schulter genommen. So hatten 44 Prozent im Herbst 2017 noch überhaupt keine Maßnahmen gestartet. Insbesondere im Mittelstand waren 39 Prozent der Befragten sehr skeptisch, alle Anforderungen und Prozesse rechtzeitig umsetzen zu können. Der Nachholbedarf ist hier folglich sehr groß – und wird auch über den Mai 2018 bestehen.

Aus Sicht von IDC ist die zögerliche Haltung in vielen Unternehmen grob fahrlässig. Die Vorbereitungen müssen daher in den kommenden Monaten vielerorts intensiviert werden. Der vorliegende Executive Brief ordnet die Handlungsfelder und Anforderungen der DSGVO ein und beleuchtet anschließend im Detail, warum der Schutz dokumentenbasierter Prozesse und Peripheriegeräte wie Drucker und Multifunktionsgeräte (MFPs) für die DSGVO-Compliance erforderlich ist – und wie er gelingen kann.

DIE WICHTIGSTEN HANDLUNGSFELDER UND ANFORDERUNGEN DER DSGVO

Nicht alle Anforderungen der DSGVO sind für Unternehmen in Deutschland grundlegend neu. Einige kommen bereits in ähnlicher Form im bestehenden Bundesdatenschutzgesetz (BDSG) vor. Dennoch müssen Unternehmen die neuen Anforderungen im Detail verstehen, um Neuerungen zu bewerten, Lücken beim Datenschutz zu identifizieren und Handlungsmaßnahmen ableiten zu können. Zudem befinden sich personenbezogene Informationen wie Kundendaten, Mitarbeiterinformationen oder Lieferantenkontakte in allen Unternehmensteilen. Die DSGVO betrifft somit das gesamte Unternehmen und erfordert eine umfassende Herangehensweise.

IDC gliedert die Anforderungen der DSGVO in die vier Handlungsfelder Technologien, Prozesse, Organisation und Recht, wobei deren Übergänge als fließend betrachtet werden können. Zu den wichtigsten DSGVO-Anforderungen in den vier Bereichen zählen beispielsweise die folgenden:

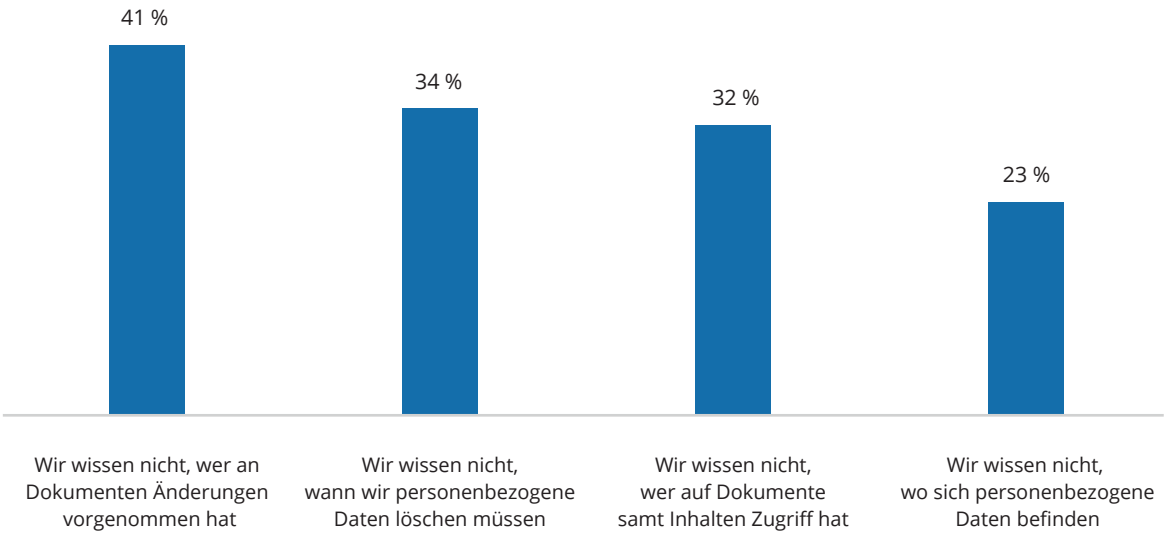
- **Technologien:** Beim Einsatz von Technologien, die personenbezogene Daten verarbeiten, muss der „Stand der Technik" berücksichtigt werden. Der Datenschutz soll zudem von Beginn an – bspw. bereits bei der Anwendungsentwicklung – integriert werden („Privacy by Design and by Default").
- **Prozesse:** Abläufe sind festzulegen, damit Unternehmen eine Datenpanne innerhalb von 72 Stunden nach deren Aufdeckung an die Aufsichtsbehörde melden. Eine absolute Transparenz bei Verarbeitungsprozessen personenbezogener Daten ist erforderlich. Zudem muss das Prinzip der Datenminimierung berücksichtigt werden.
- **Organisation:** Die Bestellung eines Datenschutzbeauftragten ist erforderlich, der für die Überwachung und Einhaltung der DSGVO verantwortlich ist.
- **Recht:** Das „Recht auf Vergessenwerden" verlangt von Unternehmen, personenbezogene Daten unwiderruflich zu löschen und dies auch zu belegen. Zudem ist eine „gesonderte Einwilligung pro Verwendungszweck" von den betroffenen Personen erforderlich.

Die genannten Anforderungen verdeutlichen, dass eine detaillierte Auseinandersetzung mit der DSGVO dringend geboten ist. Die folgenden Abschnitte fokussieren sich auf die Handlungsfelder Technologien und Prozesse und bieten einen tieferen Einblick, wie Unternehmen personenbezogene Daten in Dokumenten, Workflows und Output-Geräten schützen können.

TRANSPARENZ ALS WESENTLICHE VORAUSSETZUNG FÜR DIE DSGVO-COMPLIANCE

Für die Einhaltung der Compliance ist der ganzheitliche Überblick über die personenbezogenen Daten im Unternehmen eine Grundvoraussetzung. Unternehmen sind in der Pflicht, absolute Transparenz in Bezug auf die Daten zu schaffen. Egal, ob sich personenbezogene Informationen in Dokumenten, Datenbanken oder auf Druckerfestplatten befinden. Zudem können Verantwortliche Firmendaten nur schützen, wenn sie diese auch kennen. Bei einem Audit durch eine Aufsichtsbehörde müssen Unternehmen in der Lage sein, beispielsweise folgende Fragen zu beantworten und zu belegen: Welche personenbezogenen Daten haben wir? Wo werden sie gespeichert? Haben wir die Einwilligung, sie zu nutzen? Wer kann auf sie zugreifen? Wie lange dürfen die Daten gespeichert werden?

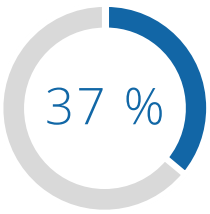
Abbildung 1: Unternehmen kennen ihre Daten und Dokumente nicht gut genug
Aussagen zur Datentransparenz in Unternehmen



N = 234–250; ohne "Weiß nicht"; Abbildung gekürzt; Prozentwerte spiegeln Häufigkeit der Zustimmung wider

Quelle: IDC, 2017

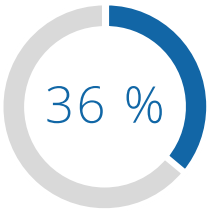
Die Befragungsergebnisse liefern ein ernüchterndes Bild hinsichtlich der Datentransparenz in Unternehmen. Zweifelsohne würden die befragten Unternehmen es bei einer Prüfung sehr schwer haben. Erschreckend, aber zugleich auch diese Einschätzung untermauernd ist, dass in 37 Prozent der Unternehmen Dokumente unkontrolliert auf den Fileservern unter der Obhut der Mitarbeiter liegen. Es ist daher dringend an der Zeit, dem vollständigen Überblick über personenbezogene Daten im Unternehmen eine höhere Priorität einzuräumen. Aufgrund der steigenden Datenmengen wird es umso wichtiger, die Daten in den Griff zu bekommen und letztlich Datenverarbeitungsprozesse stärker automatisieren zu können.



der befragten Unternehmen lassen Dokumente unkontrolliert auf Fileservern unter der Obhut der Mitarbeiter liegen.

DOCUMENT MANAGEMENT SOFTWARE KANN ORDNUNG IN DEN DATENDSCHUNGEL BRINGEN

Das Schaffen von Transparenz erfordert eine Justierung bzw. Neugestaltung von dokumentenbasierten Prozessen und Workflows im Unternehmen. Document Management Software ist hierfür ein zentraler Baustein, damit Dokumente und deren Inhalte so verarbeitet werden, dass sie den Anforderungen der DSGVO entsprechen.



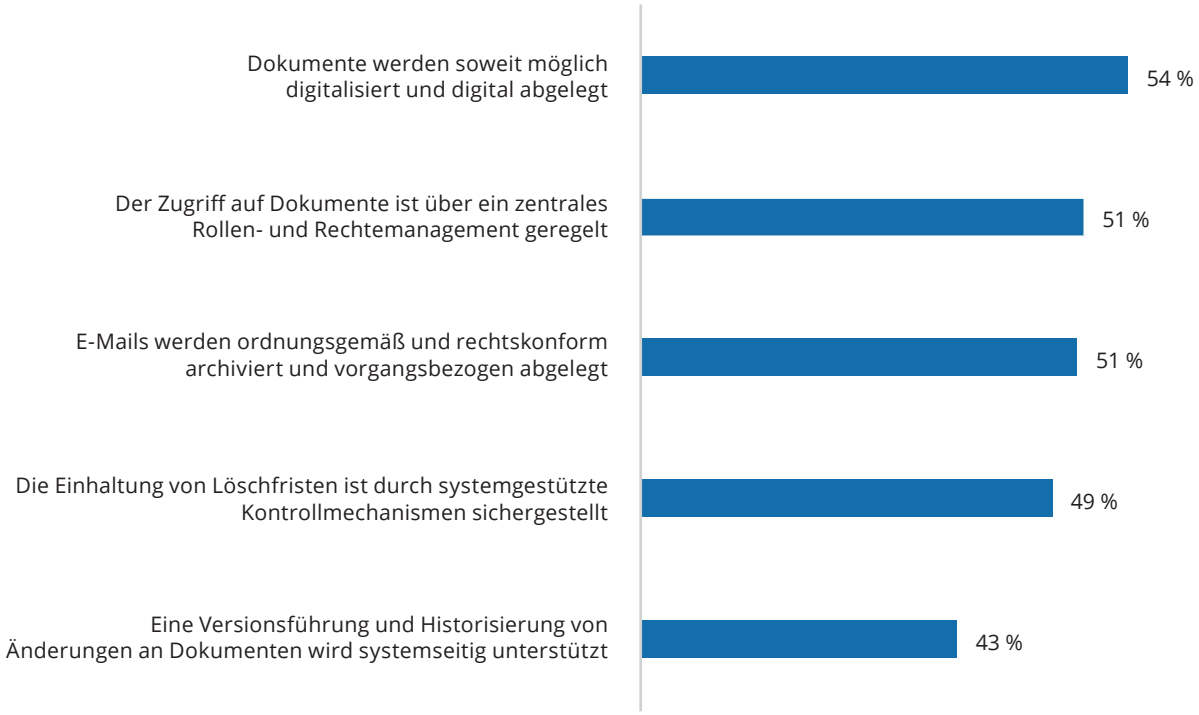
der befragten Unternehmen wollen aufgrund der DSGVO ihre Ausgaben für Document Management Software erhöhen.

Eine wesentliche Herausforderung ist dabei, dass personenbezogene Daten sowohl in strukturierter als auch in unstrukturierter Form vorliegen können. Letzteres ist beispielsweise bei Dokumenten oder E-Mails der Fall. Die DSGVO greift hier ebenso und Anforderungen müssen entsprechend eingehalten werden. Unternehmen sollten daher auf Document Management Software setzen, die diese Anforderungen nach dem aktuellen Stand der Technik erfüllt.

Im Kontext der DSGVO heben Unternehmen die Digitalisierung, Archivierung, Verwaltung und Zugriffsrechteverteilung als wesentliche Funktionalitäten ihres Dokumentenmanagements hervor. Insgesamt wird Document Management Software von Unternehmen jedoch noch nicht ausreichend eingesetzt. 36 Prozent der befragten Unternehmen wollen allerdings ihre Ausgaben für entsprechende Lösungen aufgrund der DSGVO ausweiten.

Abbildung 2: Mehrwerte von Document Management Software zur DSGVO-Compliance

Die häufigsten Anwendungsfälle von Document Management Software



N = 251; Abbildung gekürzt

Quelle: IDC, 2017

Ein wesentlicher Treiber hierfür ist auch die Festlegung und Automatisierung von Prozessen. Unternehmen sind durch die DSGVO dazu verpflichtet, bestehende datenschutzrelevante Prozesse zu überprüfen, diese an die neuen Anforderungen anzupassen oder neu einzuführen. Zu den notwendigen Workflows zählen beispielsweise die Datenlöschung nach Widerruf, die Auskunft an betroffene Personen bei Datenänderungen oder die Dokumentation der Zugriffsrechte. Unternehmen sind durchaus aufgeschlossen, hierfür auch auf Document Management Software zurückzugreifen. So wollen in 2018 beispielsweise 35 Prozent der Befragten durch entsprechende Lösungen die Einhaltung von Löschfristen sicherstellen. Aus Sicht von IDC sollten sie sehr genau prüfen, welche Prozesse relevant sind und wie diese Prozesse in IT-Lösungen abgebildet werden können. Denn die Automatisierung von Prozessen sichert Nachvollziehbarkeit sowie eine konsistente und schnelle Bearbeitung von Aufgaben.

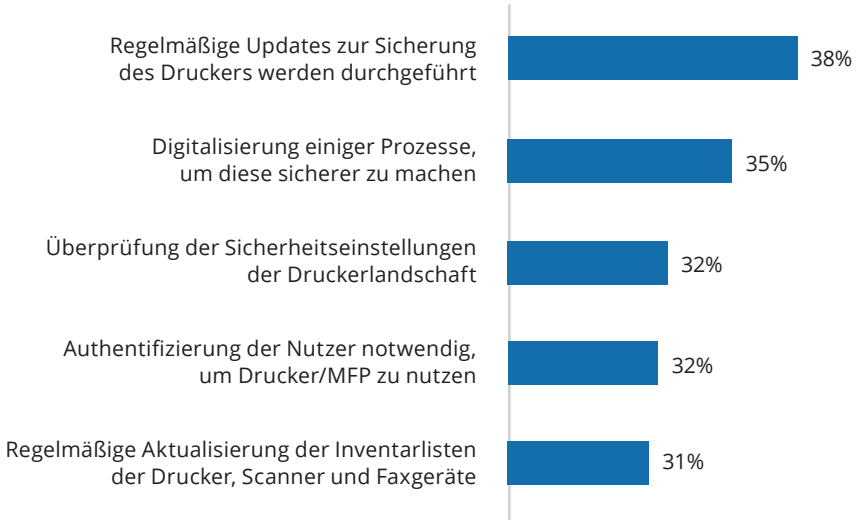
DRUCKER UND MFPS SIND NOCH ZU HÄUFIG UNTER DEM „DSGVO-RADAR"

Doch vielerorts sind die Voraussetzungen für eine stärkere Automatisierung noch nicht ausreichend geschaffen. Denn nach wie vor ist der Anteil nicht-digitalisierter Dokumente und Workflows in Unternehmen beachtlich. IDC erwartet, dass das papierlose Büro auch in den kommenden Jahren eine Illusion bleibt. Papierbasierte Dokumente mit personenbezogenen Daten, wie eine Lieferantenrechnung, Kundenbestellung oder Reisekostenabrechnung, sind daher auch unbedingt im Kontext der DSGVO zu berücksichtigen.

Papierdokumente stellen für Unternehmen eine große Herausforderung dar, da die Lokalisierung und Identifizierung der Daten besonders aufwändig ist. Beispielsweise muss ein Unternehmen durch das „Recht auf Vergessenwerden" sämtliche personenbezogenen Daten des Betroffenen löschen – egal, ob diese digital oder in Papierform bspw. in Akten vorliegen. Diese Aufgabe manuell durchzuführen ist natürlich sehr zeit- und kostenintensiv und ein wesentlicher Grund, warum Unternehmen verstärkt Document Management Software zur Digitalisierung, Archivierung und Automatisierung einsetzen wollen.

Darüber hinaus muss der Schutz personenbezogener Daten auf Papier bereits am Entstehungsort – dem Drucker oder Multifunktionsgerät – beginnen. Hier bieten moderne Geräte beispielsweise Funktionen, die eine Authentifizierung der Nutzer verlangen oder verhindern, dass Dokumente liegen gelassen werden. Etwa jedes vierte Unternehmen nimmt diese Maßnahmen derzeit in Anspruch. Doch auch die Drucker und MFPs selbst, die zum Beispiel digitale Druckversionen eines Dokuments auf der internen Festplatte speichern, müssen geschützt werden. Jedes sechste Unternehmen äußerte, dass Drucker, Scanner oder MFPs von Cyber-Kriminellen in der Vergangenheit als Einstiegspunkt genutzt wurden, da auf vorhandene Sicherheitsmöglichkeiten nicht zurückgegriffen wurde. Dies sollte in Hinblick auf die DSGVO aufhorchen lassen.

Abbildung 3: Viel Luft nach oben beim Schutz personenbezogener Daten bei Druckern und Scannern
Verbreitung von Maßnahmen zum Schutz personenbezogener Daten an Druckern/MFPs



N=251, Mehrfachnennungen; Abbildung gekürzt

Quelle: IDC, 2017

Allerdings befinden sich Drucker, MFPs und deren Netzwerk bei den DSGVO-Vorbereitungen häufig „unterhalb des Radars". Ihre Absicherung rangiert aus Sicht der Befragten lediglich auf Rang 16 der wichtigsten IT-Security-Initiativen. Die niedrige Verbreitung von Maßnahmen zur Druckersicherheit wie regelmäßige Updates, Checks der Sicherheitseinstellungen, Authentifizierung am Gerät oder eine kontinuierliche Pflege der Inventarlisten untermauern diese Einschätzung.

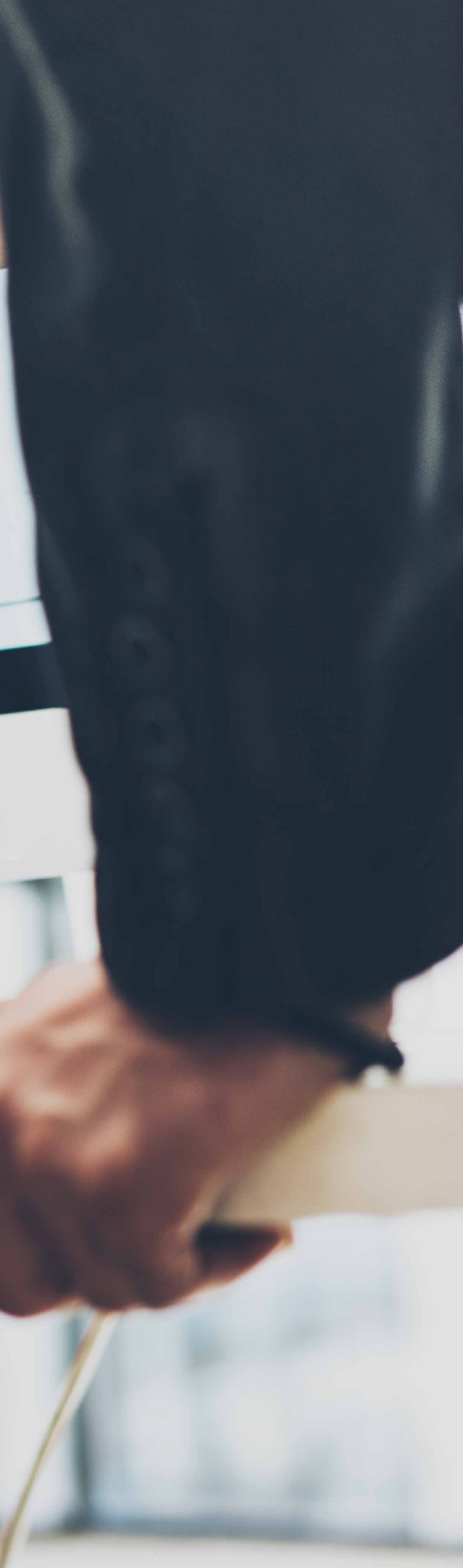
Dies ist aus Sicht von IDC grob fahrlässig. Offenkundig schenken Unternehmen dem Schutz personenbezogener Daten im Print-Umfeld noch nicht ausreichend Beachtung. Zudem verlassen sich nicht wenige Firmen blindlings auf ihre Managed Print Service Provider, ohne mit ihnen Aufgaben und Verantwortlichkeiten in Hinblick auf die DSGVO abgestimmt zu haben. Der Print Security sollte daher aus IDC Sicht ein deutlich höherer Stellenwert auf der Agenda für die DSGVO-Compliance in den kommenden Monaten zugewiesen werden. Die technologischen Möglichkeiten sind größtenteils am Markt verfügbar. Entscheider stehen nun in Hinblick auf zukünftige Datenschutz-Audits in der Pflicht, diese tatsächlich auch zu ergreifen.

FAZIT

Unternehmen in Deutschland beschäftigen sich seit vielen Jahren mit der Einhaltung des Datenschutzes und der Verbesserung der Datentransparenz. Nicht zuletzt, um die bisherigen Anforderungen des BDSG zu erfüllen und die Voraussetzungen für funktionierende Prozesse zu schaffen. Die bis dato unzureichende Umsetzung der EU-Datenschutz-Grundverordnung zeigt allerdings, dass zahlreiche Unternehmen ihre gute Ausgangslage nicht genutzt haben.

Zweifelsohne ist der Weg zur DSGVO-Compliance kein einfacher. Es bedarf eines ausgereiften Zusammenspiels an Technologien und Prozessen, um den Anforderungen der DSGVO gerecht zu werden. Document Management Software kann hierbei einen wichtigen Beitrag zum Schutz personenbezogener Daten leisten, beispielsweise bei der Archivierung oder der Durchsetzung von Zugriffsrechten. Es ist für Unternehmen dennoch dringend erforderlich, bestehende Lücken in Hinblick auf die DSGVO zu identifizieren und zu schließen. Hierzu zählen häufig Drucker und MFPs, die oftmals zu wenig Beachtung finden. Schutzmaßnahmen für die Geräte sind am Markt verfügbar. Es ist höchste Zeit, diese zu implementieren.

Die wachsende Menge personenbezogener Daten und deren vielfältige Nutzung werden die Komplexität und die Anforderungen an den Datenschutz in den nächsten Jahren weiter steigen lassen. Die Gewährleistung der DSGVO-Compliance ist somit eine fortlaufende Aufgabe – auch über den Stichtag im Mai 2018 hinaus. Dennoch sollte sie mehr sein als nur lästige Pflicht. Die transparente Verarbeitung personenbezogener Daten erleichtert und fördert die Digitalisierung und Automatisierung vieler Geschäftsprozesse. Unternehmen sollten die DSGVO daher auch als Möglichkeit begreifen, ihre Wettbewerbsfähigkeit zu erhöhen.



IDC EMPFEHLUNGEN

1 Starten Sie mit einer Bestandsaufnahme – und beziehen Sie Drucker, MFPs und Scanner mit ein

Nicht alle Anforderungen der DSGVO sind gänzlich neu. Arbeiten Sie die Unterschiede und Handlungsfelder für Ihr Unternehmen heraus. Beziehen Sie dabei unbedingt auch die Druckhardware und die -netzwerke mit ein. Prüfen Sie hier im Detail, welche Aufgaben bei Ihrem MPS Provider liegen, und legen Sie Verantwortlichkeiten fest. Die aufgedeckten Handlungsfelder sollten Sie unverzüglich angehen.

2 Sorgen Sie für absolute Transparenz bei der Verarbeitung von personenbezogenen Daten

Sie müssen Ihre Daten kennen, um diese compliancekonform managen zu können. Es ist daher wichtig, diese zu identifizieren, zu klassifizieren sowie ihren Fluss zu erfassen und wenn nötig neu zu justieren. Dokumente spielen hierbei eine wichtige Rolle. Stellen Sie durch entsprechende Software-Lösungen sicher, dass Sie die DSGVO-Anforderungen nach Transparenz und Dokumentation erfüllen.

3 Stellen Sie ein Team zusammen, das die DSGVO-Umsetzung auch nach dem Mai 2018 gewährleistet

Bringen Sie IT-Entscheider, Fachbereichsleiter, Rechtsexperten und den Datenschutzbeauftragten zusammen. Das Team hat die Aufgabe, eine zügige und anhaltende DSGVO-Compliance zu gewährleisten. Hierzu zählen insbesondere die Umstellung von Prozessen, die Einführung neuer Technologien, die Dokumentation der Maßnahmen und deren regelmäßige Überprüfung.

METHODIK

Die Ergebnisse dieses Executive Briefs basieren unter anderem auf einer Befragung von 251 IT- und Fachbereichsverantwortlichen aus Unternehmen mit mehr als 20 Mitarbeitern in Deutschland, die im Herbst 2017 durchgeführt wurde. Die Stichprobe setzt sich aus den wesentlichen Branchen der deutschen Wirtschaft zusammen.

Für weitere Informationen bezüglich dieser Veröffentlichung kontaktieren Sie bitte:
Katja Schmalen, Marketing Director, +49 69 90502-115 oder kschmalen@idc.com.

IDC CENTRAL EUROPE GMBH

Hanauer Landstr. 182 D
60314 Frankfurt • Germany
T: +49 69 90502-0
F: +49 69 90502-100
E: info_ce@idc.com
www.idc.de

IDC
ANALYZE THE FUTURE