IDC Executive Brief

Gesponsert von: **Brother**

Autor:

Jacqui Hendriks

März 2018

Gewährleistung des Datenschutzes: Die wachsende Herausforderung im Print- und Dokumentenmanagement

Viele Unternehmen werden die neuen Datenschutz- und Sicherheitsvorschriften nicht einhalten, weil sie potenzielle druckbezogene Schwachstellen übersehen haben. Eine ungesicherte Druckumgebung ist eine ungesicherte IT-Umgebung.

Der IDC Executive Brief bietet eine Einführung in die neuen Datenschutzgesetze, die erforderlichen Initiativen zu Erfüllung der Compliance und die spezifischen Maßnahmen, die erforderlich sind, um Druck- und Dokumentenmanagementprozesse konform zu gestalten.

Schutz von Kundendaten

Angetrieben durch technologische Innovationen hat sich die Art und Weise, wie Unternehmen aller Größenklassen Informationen erhalten, verarbeiten, konsumieren und liefern, dramatisch verändert. Die Unternehmen erhalten exponentielle Informationsmengen in gedruckter und elektronischer Form. Untersuchungen von IDC zeigen, dass die Menge der erstellten, erfassten und replizierten Daten bis 2025 auf 163 Zettabyte (ZB) oder 163 Billionen Gigabyte (GB) steigen werden. Dies entspricht dem Zehnfachen der 16,12 ZB an Daten, die im Jahr 2016 erstellt wurden[1]. Doch das Datenschutzgesetz hinkt hinter diesen sich wandelnden Verhaltensweisen am Arbeitsplatz hinterher.

Die Fähigkeit, diese Informationen zu erfassen, kann dazu beitragen, Kunden zu gewinnen und zu binden, indem die Kundenerfahrung verbessert wird[2]. Aufgrund eines ineffizienten Informationsmanagements fällt es den Unternehmen bereits oft schwer, die Informationen zu finden[3.] Insbesondere, wenn Informationen nicht richtig verwaltet werden besteht ein erhöhtes Risiko, dass sensible Daten in die falschen Hände geraten. Dies kann zu erheblichen Datenverletzungen führen, die die persönlichen Daten der Öffentlichkeit/Kunden gefährden.

Zu den besonders anfälligen Punkten zählen:

- Unsachgemäße Verwendung von Druckgeräten und Druckausgaben
- Daten auf internen Gerätespeichern
- Potenzielle Verstöße durch Netzwerk-Ports an den Geräten
- Nicht abgeholte Dokumente

Das Datenschutzgesetz wird derzeit aktualisiert, um die heutigen Verhaltensweisen und Werte, einschließlich der Nutzung von sozialen Medien und anderen Onlinediensten, zu reflektieren. Die EU-Datenschutzrichtlinie

(95/46/EG) aus dem Jahr 1995 stammt aus einer Zeit vor der Existenz vieler aktueller Online-Geschäftsmodelle und vor der Einführung von Cloud- und Social-Media-Services. Die neuen Rechtsvorschriften verhängen erhebliche Strafen gegen jene Unternehmen, die keine konzertierten Anstrengungen unternehmen, um das Risiko zu reduzieren.

Derzeit steht die Datenschutz-Grundverordnung (DSGVO) 2016/679 der Europäischen Union (EU) im Mittelpunkt, aber es gibt viele weitere neue europäische Rechtsvorschriften in Bezug auf den Datenschutz in der EU, z. B.[4]:

Derzeit steht die Datenschutz-Grundverordnung (DSGVO) 2016/679 der Europäischen Union (EU) im Mittelpunkt, aber es gibt viele weitere neue europäische Rechtsvorschriften in Bezug auf den Datenschutz in der EU.

- **Richtlinie 2016/680** – Sie wird als Zwilling der DSGVO angesehen und konzentriert sich auf die Verarbeitung von personenbezogenen Daten zur Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten oder strafrechtlichen Verfolgungen. Dies war zuvor eine Richtlinie, die ab dem 6. Mai 2018 in den 28 EU-Mitgliedstaaten in nationale Gesetze umgesetzt wird.
- **Die Richtlinie über Netz- und Informationssicherheit (NIS)** – Diese Richtlinie wurde von der EU verabschiedet, um einen einheitlichen Ansatz gegen Cyber-Angriffe auf wesentliche Dienstleistungen wie Energie, Verkehr, Banken, Finanzmarktinfrastruktur, Gesundheit, Trinkwasserversorgung, digitale Infrastruktur und digitale Dienste einzuführen.
- **Die ePrivacy-Verordnung** – Zusammen mit der DSGVO bildet die ePrivacy-Richtlinie (ePD) den Rechtsrahmen für die digitale Privatsphäre der EU-Bürger und betrifft die Kommunikation über öffentliche Netzwerke. Die ePD stammt aus dem Jahr 2002, wird aber überarbeitet, um sie auf den neuesten Stand der Technik zu bringen.
- **Die Richtlinie über die Verwendung von Fluggastdatensätzen (PNR-Daten)** – Diese bezieht sich auf die übliche Praxis der Erfassung von Passagierdaten vor dem Abflug. Die EU-Mitgliedstaaten müssen die Richtlinie bis zum 24. Mai 2018 in nationales Recht umsetzen. Personenbezogene Daten, die als PNR-Daten gesammelt werden, müssen sechs Monate lang gespeichert werden. Danach müssen die Daten anonymisiert und dann für einen weiteren Zeitraum von viereinhalb Jahren gespeichert werden.

Während einige der neuen Rechtsvorschriften relativ allgemein oder hochgradig branchenspezifisch sind, werden sich alle darauf auswirken, wie Unternehmen in Zukunft gedruckte Dokumente und Dokumentenworkflows verwalten.

Datenschutz und Sicherheit

Die DSGVO 2016/679 definiert eine Datenverletzung als „zufällige oder unrechtmäßige Zerstörung, Verlust, Veränderung, unberechtigte Offenlegung von oder den Zugriff auf persönliche Daten, die übertragen, gespeichert oder anderweitig verarbeitet wurden." Sie stellt einen grundlegenden Wandel in den EU-Gesetzen zum Schutz der personenbezogenen Daten der EU-Bürger dar. Dies betrifft auch internationale Unternehmen außerhalb der EU,

einschließlich der britischen Unternehmen nach dem Brexit, die Daten von EU-Bürgern verwalten.

Die Begründung für die DSGVO liegt in zwei primären Zielen. Das erste besteht darin, das Datenschutzrecht auf den neuesten Stand zu bringen, und das zweite ist die Harmonisierung der EU-Datenschutzvorschriften in einem einzigen Gesetz. Es beruht auf der Prämisse, dass:

- Die Unternehmen keine eigenen Daten besitzen. Die neueste Gesetzgebung unterstützt das Recht der Öffentlichkeit, zu wissen, ob ihre Daten korrekt gehandhabt werden, und informiert zu werden, wenn sie verloren gehen, gestohlen oder anderweitig missbraucht werden, wenn eine solche Verletzung ein hohes Risiko für sie darstellt (obligatorische Benachrichtigung bei Sicherheitsverletzungen).
- Die Unternehmen müssen sich an das „Recht auf Vergessen" der Öffentlichkeit halten. Um dies zu erreichen, müssen die Unternehmen wissen, wo sich die Daten zu einem bestimmten Thema befinden – in welcher Anwendung oder auf welchem Gerät. Darüber hinaus ist es erforderlich, dass alle Informationen in einer standardisierten Weise in alle Datenarchive in sämtliche Systeme/Plattformen/Geräte eingebunden werden.

Die DSGVO stellt die Frage der Print- und Dokumentensicherheit und der Datensicherheit in den Fokus. Es wird gefordert, dass für alle gedruckten und elektronischen Arbeitsabläufe bestimmte Bedingungen erfüllt werden müssen. Korrekt dokumentierte Prozesse und adäquate Aufzeichnungen, Protokolle und Prüfpfade helfen bei der Behebung von Sicherheitsverletzungen; aber, wenn ein Verstoß vorliegt, gibt es Hinweise darauf, dass adäquate Maßnahmen getroffen wurden, um den Verstoß zu vermeiden.

Viele der Anforderungen sowie die anderer bevorstehender Rechtsvorschriften sind möglicherweise deutlich strenger als das Gesetz, das sie ersetzen. Bußgelder für die Nichteinhaltung sind absichtlich hoch – „wirksam, verhältnismäßig und abschreckend" in der DSGVO – aber das zugrundeliegende Ziel ist es, den Weg zur Compliance für alle Beteiligten klar und einfach zu machen. Der Nachweis der Absicht eines Unternehmens und seiner Bemühungen, die Vorschriften zu erfüllen, fällt stark ins Gewicht, wenn die zuständige Behörde eine Sicherheitsverletzung untersuchen muss.

Die Nichteinhaltung kann schwerwiegende negative Auswirkungen auf das Image eines Unternehmens haben. In der Tat ist das Reputationsrisiko durch die Nichteinhaltung eines der wichtigsten Bedenken im Zusammenhang mit der DSGVO[5].

Bei der Erfüllung der Compliance-Anforderungen haben Unternehmen vier zentrale Investitionsprioritäten[6]:

- Identifizierung der Anwendungen, die Daten verwenden, für die spezifische Compliance-Vorschriften gelten.
- Datenzuordnung und Ermittlung – Bewertung und Klassifizierung von Daten
- Festlegung von Dokumentationsprozessen
- Überprüfung und Verbesserung der Identitäts- und Zugangsverwaltung (Identity and Access Management)

Die DSGVO stellt die Frage der Print- und Dokumentensicherheit und der Datensicherheit in den Fokus. Es wird gefordert, dass für alle gedruckten und elektronischen Arbeitsabläufe bestimmte Bedingungen erfüllt werden müssen. Es muss ein Prüfpfad vorliegen, der Zugriff und die Verarbeitung müssen

autorisiert sein, und Informationen müssen gesichert sein, einschließlich der Daten, die auf Druckgeräten gespeichert sind. Korrekt dokumentierte Prozesse und adäquate Aufzeichnungen, Protokolle und Prüfpfade tragen dazu bei, Sicherheitslücken zu schließen; aber, wenn ein Verstoß vorliegt, gibt es Hinweise darauf, dass adäquate Maßnahmen getroffen wurden, um den Verstoß zu vermeiden.

Anbieter von Druck- und Dokumentenmanagement haben sich verpflichtet, die Datenschutzbestimmungen einzuhalten und sind gut positioniert, um ihre Kunden zu unterstützen. Letztendlich liegt es jedoch in der Verantwortung jedes einzelnen Unternehmens, die Rechtsvorschriften einzuhalten.

Bis heute scheinen die Unternehmen den notwendigen drucktechnischen Anforderungen nicht gerecht zu werden, denen sie gerecht werden müssen, ohne sich über die Gesetzgebung, ihre Auswirkungen und die damit verbundenen zeitlichen Vorgaben im Klaren zu sein[7]:

- Trotz der Tatsache, dass 2018 Bußgelder rechtswirksam werden, wussten 40 % der Druckauftraggeber Anfang 2017 nicht, was DSGVO ist. Weitere 19 % kannten die Verordnung, jedoch nicht die zeitlichen Rahmenvorgaben. Die Unternehmen, die sich dessen bewusst waren, wiesen allgemein entspannte Vorgehensweisen auf, waren aber dennoch zuversichtlich, dass die Compliance erreichbar ist.
- Noch überraschender war, dass von den Druckauftraggebern, die wussten, was DSGVO ist, 51 % nicht klar war, dass die Verordnung signifikante Auswirkungen auf das Druckgeschäft hat.

Einhaltung der Rechtsvorschriften für Print- und Dokumentenmanagement

Von den Druckauftraggebern, die wussten, was DSGVO ist, war 51 % nicht klar, dass die Verordnung signifikante Auswirkungen auf das Druckgeschäft hat.

Die Betriebssicherheit ist für alle Unternehmen von höchster Priorität – von Einzelhändlern bis hin zu großen multinationalen Unternehmen. Die drei sicherheitsrelevantesten Herausforderungen sind[7]:

1. Geschäftskontinuitäts- und Disaster-Recovery-Planung
2. Immer ausgefeilteren Angriffen stets einen Schritt voraus sein
3. Compliance und Einhaltung dringender Vorschriften

Trotz zunehmender Vorfälle von durchgesickerten Unternehmens- und personenbezogenen Daten, wird bei der Drucksicherheit nicht genügend darauf geachtet, was zu tun ist, um die Rechtsvorschriften einzuhalten[7].

- Die Investitionen in Drucksicherheit sind gering – mehr als die Hälfte der Unternehmen geben weniger als 3 % ihres IT-Sicherheitsbudgets für Drucksicherheit aus.
- Die Zukunftspläne zeigen, dass zwei Drittel der Unternehmen in den nächsten 12 Monaten keine Erhöhung der Ausgaben beabsichtigen und nur ein Drittel die Drucksicherheit in die Angebotsanfragen für IT-Technologie aufnimmt.

Es wurden bereits Lösungsangebote entwickelt, die sowohl die Effizienz der Print- und Dokumentenverwaltung von Unternehmen verbessern als auch die Herausforderung der Einhaltung von Datenschutzbestimmungen meistern:

- Die Unternehmen zeigten, dass sie sehr daran interessiert sind, sichere Druckfunktionen – zum Beispiel Drucken auf Abruf und authentifizierte und autorisierte Endbenutzerlösungen – in ihre Multifunktionsdrucker (MFD) zu integrieren[3]. Infolgedessen können Unternehmen basierend auf der Rolle und Verantwortung der Mitarbeiter den Zugang zu bestimmten Informationen einschränken. Dies stellt eine zuverlässige Compliance-Maßnahme zur Risikominimierung dar. Die steigende Nachfrage, Informationen zur Integration in den elektronischen Dokumentenworkflow zu digitalisieren, hat zu einer erhöhten Verwendung von Scannern geführt. Nach einer Umfrage von IDC in 2017 zu den Druckgewohnheiten in Europa ist direktes Scannen an E-Mails, Netzwerkordner und bestehende Systeme (z. B. ERP, CRM) für Unternehmen heutzutage von großem Interesse. Darüber hinaus gibt es eine größere Nachfrage nach intelligenten MFPs, die Scanfunktionalität und den direkten Zugriff auf gespeicherte Daten bieten[3].

Die Bereitstellung von einem effektiven sicheren Druck- und Dokumentenmanagement wurde von Print- und Imaging-Anbietern nicht vernachlässigt. Sie bieten eine breite Palette von Lösungen an, die Unternehmen dabei unterstützen, den Compliance-Prozess zu optimieren, ohne dabei wichtige Ressourcen von umsatzsteigernden Aktivitäten abzuziehen:

- **Printmanagement- und Monitoring-Lösungen –** Dies sind effektive Werkzeuge für das Tracking und die Berichterstattung der Gerätenutzung zur Bewertung der Druckumgebungen bei Vertrags-/Kaufverhandlungen. Aus diesem Grund setzen mehr als die Hälfte der Unternehmen (53 %) diese Lösungen ein[8]. Zudem bieten sie den Mehrwert, einen Prüfpfad zu erstellen, um zu ermitteln, was ausgedruckt/bearbeitet wird, wo und von wem. Diese Fähigkeit, einen Prüfpfad zu erstellen, ist ein wesentlicher Bestandteil bei der Schadensbegrenzung größerer Sicherheitsverletzungen.
- **Sicherer Zugang und Authentifizierung –** 46 % der Unternehmen verlangen, dass sich Mitarbeiter zur Anmeldung bei einem Druckergerät[8] vor der Nutzung mit einem PIN-Code oder per Near Field Communication (NFC) ausweisen. Diese Funktionalität ist oft nur für Abteilungen verpflichtend, die in erster Linie sensible Materialien verarbeiten, wie etwa das Personalwesen sowie die Rechts- und Finanzabteilung.
- **Sicherer Druckzugriff mit Active Directory –** Dies sorgt durch die Sperrung von physischen Gerätefunktionen für noch mehr Sicherheit und ermöglicht zudem eine größere Flexibilität, wie beispielsweise die Festlegung einer Frist für die Abholung von Druckaufträgen.

Die Bereitstellung eines effizienten, sicheren Druck- und Dokumentenmanagements wurde von Print- und Imaging-Anbietern nicht vernachlässigt. Sie bieten eine breite Palette von Lösungen, die den Unternehmen helfen, den Prozess der Compliance zu optimieren.

Dokumente, die nicht auf dem Gerät abgerufen wurden, können ein Risiko darstellen, wenn sie missbräuchlich abgefangen werden.

- **Sicherheit von Druckgeräten –** Unternehmen sind zunehmend besorgt, dass vertrauliche Unternehmensinformationen, die auf vernetzten Peripheriegeräten gespeichert werden, unbeabsichtigt öffentlich bekannt werden können[8]. Einige Druckerhersteller sorgen dafür, dass Nutzer keine Informationen auf dem Gerät speichern können. Stattdessen können sie die Möglichkeit nutzen, Dokumente von einem zentralen sicheren Server oder einem sicheren Cloud-Speicherdienst abzurufen. Unternehmen haben daher die Sicherheit, dass Dokumente nicht von einem Gerät abgerufen werden können, wenn das Gerät physisch beeinträchtigt sein sollte.
- **Sicheres Scannen –** Sicherheitsmaßnahmen sind nicht nur auf Druckausgaben beschränkt. Gescannte Dokumente können auch als PDF-Datei mit einem PIN-Zugangscode oder durch ein sicheres Datenübertragungsprotokoll (Secure File Transfer Protocol; SFTP) gesichert werden, um einen sicheren Datenstroms zu erstellen. 20 % der Unternehmen haben Sicherheitsbedenken bezüglich der Zugriffsberechtigung auf gescannte Dokumente für Mitarbeiter[9].
- **Sichere Datenkommunikation –** Geräte, die zum Drucken, Scannen oder für andere Dokumentenverwaltungsaufgaben eingesetzt werden, sollten durch die Konfiguration von in der Branche anerkannten Sicherheitsmerkmalen wie Internet Protocol Security (IPSEC) und Transport Layer Security (TLS) gesichert werden. Diese Funktionen sorgen dafür, dass die Kommunikation zum und vom Gerät authentifiziert, vertrauenswürdig und vertraulich ist.
- **Netzwerkbedrohungen –** Unternehmen müssen dafür sorgen, dass das Druckgerät keine Schwachstelle darstellt, indem die gleiche Sicherheitsstufe wie bei anderen IT-Geräten, wie Laptops und Tablets, angewandt wird.

Anstatt den Weg zur Compliance als eine hohe Belastung anzusehen, sollten Unternehmen diesen als Chance sehen, um bessere Prozesse zu implementieren.

Einfachere Workflows helfen ihnen nicht nur, die Vorgaben zu erfüllen, sondern tragen generell dazu bei, Informationen täglich effizienter zu verarbeiten. Darüber hinaus können bei der Implementierung besserer Prozesse zur Einhaltung der Compliance Kosteneinsparungen ein Nebeneffekt sein.

Bei der Implementierung besserer Prozesse zur Einhaltung der Compliance können Kosteneinsparungen ein Nebeneffekt sein.

Anleitung: Einhaltung der Compliance-Vorschriften für Druck- und Dokumentenmanagement

Unternehmen, die die Sicherheit Ihrer Geschäftstätigkeit und die Einhaltung der Datenschutzbestimmungen gewährleisten möchten, sollten diese 10-Punkte-Checkliste berücksichtigen:

- ☑ Überprüfen Sie die aktuellen Sicherheits- und Datenschutzrichtlinien Ihres Unternehmens und richten Sie diese an den wesentlichen Sicherheits- und Datenschutzanforderungen aus, um sicherzustellen, dass die Druckinfrastruktur ein integraler Bestandteil dieser Überprüfung ist.
- ☑ Identifizieren Sie internes Personal mit den entsprechenden Fähigkeiten sowie potenziellen Qualifikationslücken.
- ☑ Erwägen Sie, Ihren Druckgeräteanbieter nach Ressourcen zu fragen, die die IT-Abteilung nutzen kann, um die Compliance-Initiativen zu unterstützen.
- ☑ Sichern Sie das Netzwerk, mit dem Ihre Drucker verbunden sind.
- ☑ Schützen Sie alle Arten von sensiblen Informationen, die an den/die Drucker/Scanner geschickt oder auf diesen verarbeitet werden.
- ☑ Stellen Sie sicher, dass Ihre Drucker nicht anfällig für Malware und andere Cyberangriffe sind.
- ☑ Vergewissern Sie sich, dass potenziell vertrauliche Informationen nicht auf Peripheriegeräten wie Druckern gespeichert werden.
- ☑ Implementieren Sie ein Flottenmanagement-Tool für die kontinuierliche zentrale Steuerung und Überwachung von Druck- und Scangeräten.
- ☑ Implementieren Sie eine Benutzerauthentifizierung (einschließlich Drucken auf Abruf) und -autorisierung auf dem Gerät, um ein sicheres Abrufen vertraulicher Dokumente zu gewährleisten.
- ☑ Entwickeln Sie einen nachhaltigen Plan zur Überwachung, Eskalation, Korrektur und Durchsetzung aktueller und zukünftiger Sicherheits- und Datenschutzstrategien.

Quellen:

1. *Data Age 2025: The Evolution of Data to Life-Critical, Don't Focus on Big Data; Focus on the Data That's Big*, IDC White Paper, April 2017
2. *What are the Top Priorities of LOBs and Industries in Western Europe?* IDC #EMEA43168117, Oktober 2017
3. *Content Management Opportunity: Integrated Solutions vs Outsourcing*, IDC #EMEA43165417, Oktober 2017
4. *An Overview of Incoming EU Privacy and Data Security Legislation*, IDC #EMEA42911917, August 2017
5. IDC EMEA GDPR Survey, März 2017
6. *IDC PlanScape: EU General Data Protection Regulation Compliance*, IDC #US42574817, Juni 2017
7. *Low Investment in Print Security and Increasing Compliance Challenges Leave European Companies at Risk*, IDC #EMEA42819617, Juni 2017
8. *Still Significant Opportunity to Address Print Infrastructure /Management Challenges*, IDC #EMEA43059617, September 2017
9. *Workplace Dynamics Drive Print and Document Management,* IDC #EMEA41529116, Juni 2016

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, Vereinigtes Königreich
+44 208 987 7100
Twitter: @IDC
idc-community.com
www.idc.com

Über IDC

International Data Corporation (IDC) ist der weltweit führende Anbieter von Marktinformationen, Beratungsdienstleistungen und Veranstaltungen auf den Gebieten der Informationstechnologie, der Telekommunikation und dem Consumer Markt. IDC analysiert und prognostiziert technologische und branchenbezogene Trends und Potenziale und ermöglicht ihren Kunden so eine fundierte Planung ihrer Geschäftsstrategien sowie ihres IT-Einkaufs. Durch das Netzwerk der mehr als 1100 Analysten in über 110 Ländern mit globaler, regionaler und lokaler Expertise kann IDC ihren Kunden umfassenden Research zu den verschiedensten Segmenten des IT-, TK- und Consumer Marktes zur Verfügung stellen. Seit mehr als 50 Jahren vertrauen Business-Verantwortliche und IT-Führungskräfte bei der Entscheidungsfindung auf IDC. IDC ist ein Geschäftsbereich der IDG, dem weltweit führenden Unternehmen in den Bereichen IT- Publikationen, Research und Konferenzen.