Das Drucken und die DSGVO

Zumindest bis zum Mai 2018 war sie für viele Unternehmen und Privatpersonen das Thema des Jahres: die EU-Datenschutz-Grundverordnung, kurz DSGVO. Auf lange Vorwarnzeiten folgte bei den meisten Unternehmen eine hektische Umsetzung. Dabei wurde vor allem an gestohlene Kreditkartendaten oder jahrelanges E-Mail-Marketing ohne Zustimmung der Betroffenen gedacht. Dass die DSGVO auch Auswirkungen auf die Dokumentverarbeitung und Druckprozesse hat, bedenken aber bis heute die Wenigsten.

Druckaufträge hängen in der Warteschlange, ältere Ausdrucke liegen bereits im Ausgabefach des Druckers. Dokumente über Dokumente, die personenbezogene Daten beinhalten, die, im Sinne der DSGVO, eigentlich geschützt werden müssen. Ein großes Risiko für Unternehmen, denn täglich werden Unterlagen wie Gehaltszettel, Adressetiketten für den Postversand, Leistungsnachweise und vieles mehr auf Papier gedruckt und kommen im schlimmsten Fall in Hände, für die sie nicht bestimmt sind.

Drucken mit Folgen

Dabei stellt nicht nur der physische Ausdruck ein Risiko dar. Drucker sind heute moderne kleine Computer, die gehackt werden können. Deshalb ist auch die Datenübermittlung vom Endgerät zum Drucker, die meist ohne Datenverschlüsselung erfolgt, eine DSGVO-Lücke. „Die Sicherstellung der Vertraulichkeit der in den Druckern gespeicherten personenbezogenen Daten hat Teil einer DSGVO konformen Datenschutz- und Datensicherheitsstrategie zu sein. Bei Nichtbeachtung und Kompromittierung personenbezogener Daten drohen nicht nur Strafen, sondern in gravierenden Fällen auch die Untersagung des IT-Betriebes durch die Datenschutzbehörde“, sagt Rechtsanwalt Martin Schiefer von der Kanzlei Schiefer Rechtsanwälte GmbH und erklärt weiter, „Teil dieser Strategie ist auch die sicherere Löschung der auf den Druckern noch gespeicherten Daten am Ende des Lebenszyklus.“

Voller Datendrang und passender Lösungen

Es gilt das Problem, wie so oft, an der Wurzel zu packen. Denn die Verschlüsselung der Daten, die gedruckt werden sollen, muss bereits am Endgerät und nicht erst bei der Übertragung zum Drucker oder während des Druckprozesses erfolgen. Verschlüsselte Netzwerke versprechen zumindest Abhilfe, wenn es um das Problem der unverschlüsselten Daten, die zwischen Endgerät und Drucker schwirren, geht. Sogenannte Pull-Printing-Lösungen sollen hingegen beim Dilemma der unachtsamen Mitarbeiter eingreifen. Und das nicht nur im Stammbüro und am lokalen Rechner des Mitarbeiters, sondern in jeder Filiale und an jedem Endgerät, das für berufliche Zwecke genutzt wird: Ein Mitarbeiter reist beispielsweisein eine Filiale und löst von seinem Tablet den Druck eines Dokuments aus, das er für das nächste Meeting benötigt, aber hochsensible Daten enthält. Ein Vorgang, der den Datenschutz gefährden kann. Mittels Pull Printing folgt der Druckauftrag dem Mitarbeiter überall hin und erlaubt eine freie Druckerwahl. Das Dokument wird aber erst nach Eingabe der PIN oder nach Authentifizierung mit Badge/Proximity/etc. am jeweiligen Drucker freigegeben und gedruckt, somit ist die Lösung nicht nur praktisch, sondern sorgt auch für die Einhaltung der Datenschutz-Grundverordnung. „In jedem Unternehmen werden heute mobile Geräte wie Smartphones oder Tablets eingesetzt. Pull-Printing-Lösungen erlauben es, Gerätein unternehmensweite Druckprozesse voll zu integrieren, zu steuern und alle DSGVO-Anforderungen zu erfüllen“, erklärt Karin Bopp von Levi, Ray & Shoup, Inc., Experte für Output Management. Das Unternehmen berät und unterstützt seine Kunden bei der Umstellung auf DSGVO-konforme Drucklösungen. Denn es sei höchste Zeit, bereits vorhandene Prozesse auf Sicherheitsmängel zu überprüfen und die bestehenden Mängel zu beseitigen, ist Bopp überzeugt.

> *Die Sicherstellung der Vertraulichkeit der in den Druckern gespeicherten personenbezogenen Daten hat Teil einer DSGVO-konformen Datenschutz- und Datensicherheitsstrategie zu sein. Bei Nichtbeachtung und Kompromittierung personenbezogener Daten drohen nicht nur Strafen, sondern in gravierenden Fällen auch die Untersagung des IT-Betriebes durch die Datenschutzbehörde.“*
> *Martin Schiefer, Rechtsanwalt, Schiefer Rechtsanwälte GmbH*

Text in deutscher Fassung

www.LRSOutputManagement.com