In diese fatalen DSGVO-Fallen laufen die Mitarbeiter

Mehr Selbstbestimmung im Netz, was die eigenen Daten angeht. Das ist das Ziel der neuen Datenschutzgrundverordnung. Vor allem sorgt sie für extreme Verwirrung – und viele nervige Mails.

Unternehmen müssen ihre Abläufe an die DSGVO anpassen. Doch eine große Schwachstelle für den Datenschutz sind unerfahrene oder sorglose Mitarbeiter. Die fatalsten Fehler und wie sie sich vermeiden lassen.

Quelle: WELT/ Erdmann Hummel

boldt-IT | Marcus Boldt
An der Marsch 39
29690 Gilten
Germany

Telefon: +49 5071 5215176
Telefax: +49 5071 5215175
Mobil: +49 173 69 100 11
Finanzamt Soltau | Steuer-Nr: 41/105/08516

Bankverbindung:
Hamburger Sparkasse
IBAN: DE19200505501343126874
BIC: HASPDEHHXXX

1. Akten landen im Papierkorb

Im digitalen Zeitalter wird häufig vergessen, dass auch Druck-Erzeugnisse personenbezogene Daten enthalten können. Gedruckte Dokumente und Datenträger, die im Papierkorb landen, sind vor Akten müssen ordnungsgemäß vernichtet werden (zum Beispiel schreddern). Um die gesetzlichen Vorschriften einzuhalten, ist es vorteilhaft, die Aktenvernichtung an externe Dienstleister abzugeben. Es ist einfacher, die Dokumente in Datenschutztonnen zu vernichten, als den Schredder zu benutzen.

2. Private Geräte am Arbeitsplatz

USB-Sticks, externe Festplatten und CD-ROM sind beliebt, um private Angelegenheiten am Arbeitsplatz zu erledigen oder Firmenunterlagen mit nach Hause zu nehmen, um nach der Arbeit Die Geräte können mit Schadsoftware infiziert sein, die sich im Betriebssystem ausbreitet und eine Gefahr für Daten darstellt. Betriebsintern sollten daher private Geräte verboten und firmeneigene 3. Firmengeräte werden für private Zwecke genutzt

Homeoffice und unterwegs arbeiten sind weit verbreitet. Häufig werden die zur Verfügung gestellten Arbeitsmittel (Laptops, Tablets, Smartphones) auch für private Zwecke genutzt.

Dadurch können unbefugte Drive, insbesondere bei Verlust oder Diebstahl, leicht Einblick in vertrauliche Firmenunterlagen erhalten. Festplatten und USB-Sticks sollten deshalb unbedingt verschlüsselt und die Nutzung des öffentlichen WLAN verboten werden.

4. Nutzung des privaten E-Mail-Accounts

Viele Mitarbeiter nutzen private E-Mail-Adressen zum Versenden von betrieblichen Dokumenten mit vertraulichen personenbezogenen Daten. Gründe: Bequemlichkeit, Unerfahrenheit mit E-Mail- Programmen des Unternehmens, Nutzung der Dokumente für private Zwecke.

Dabei nutzen sie häufig unsichere Transfermethoden. Leider wissen das auch viele Hacker, die immer auf der Suche nach Möglichkeiten sind, vertrauliche Daten zu stehlen.

Quelle: WELT/ Erdmann Hummel

boldt-IT | Marcus Boldt
An der Marsch 39
29690 Gilten
Germany

Telefon: +49 5071 5215176
Telefax: +49 5071 5215175
Mobil: +49 173 69 100 11
Finanzamt Soltau | Steuer-Nr: 41/105/08516

Bankverbindung:
Hamburger Sparkasse
IBAN: DE19200505501343126874
BIC: HASPDEHHXXX

Die Nutzung privater E-Mail-Accounts für betriebliche Zwecke sollte daher untersagt sein. Für die Verschlüsselung von Dateianhängen sollten automatisierte Tools eingesetzt werden.

5. Mein Passwort für alles: hallo123

Mitarbeitern, die personenbezogene Daten verarbeiten, sollten für jede Anwendung eigene Accounts eingerichtet werden. Account-Sharing ist ein No-go! Die Accounts sind allerdings sinnlos, wenn sie nicht durch sichere Passwörter geschützt sind.

Aus Bequemlichkeit werden gern einfache Passwörter genutzt und am liebsten immer das gleiche. Ein fataler Datenschutzfehler! Ist ein Passwort einmal geknackt, besteht so die Möglichkeit, auf alle Nutzer-Accounts zuzugreifen und somit Zugang zu vertraulichen Daten zu erlangen.

Mitarbeiter sollten technisch gezwungen werden, lange Passwörter (acht bis zwölf Zeichen) zu nutzen, die zudem aus Groß- und Kleinschreibung, Ziffern sowie Sonderzeichen bestehen. Diese müssen auch regelmäßig geändert werden.

6. Hereinspaziert!

Büroräume bieten einige Gefahren für Datenschutzverstöße. Insbesondere wenn betriebsfremde Personen in Büroräume gelassen werden und ohne Begleitung umherspazieren können.

Ein offenes Büro, ein unverschlossener Serverraum, ein vergessenes Dokument auf dem Drucker können fatale Folgen für den Datenschutz von Kunden und Mitarbeitern haben. Der Zugang zu den Büroräumen sollte Betriebsfremden nur für Betriebszwecke gestattet sein, und das auch nur unter Aufsicht.

7. Zu viel Auskunft am Telefon

Vor allem unerfahrenen Telefonisten kann es passieren, dass AuskünTe zu personenbezogenen Daten gegenüber einem unberechtgten Zuhörer gemacht werden. Zur Vermeidung ist es unerlässlich, den Mitarbeiter schon im Voraus gründlich darin einzuweisen, welche AuskünTe gemacht werden dürfen und welche nicht.

Quelle: WELT/ Erdmann Hummel

boldt-IT | Marcus Boldt
An der Marsch 39
29690 Gilten
Germany

Telefon: +49 5071 5215176
Telefax: +49 5071 5215175
Mobil: +49 173 69 100 11
Finanzamt Soltau | Steuer-Nr: 41/105/08516

Bankverbindung:
Hamburger Sparkasse
IBAN: DE19200505501343126874
BIC: HASPDEHHXXX

8. Chaos am Arbeitsplatz

Vertrauliche Briefe, Verträge, Notzen mit Passwörtern, USB-Sticks, und das alles auf einem Haufen. Wenn dann auch noch jeder x-beliebige Mitarbeiter diesen Haufen sehen kann, ist das

Hilfreich ist eine Clean-Desk-Policy, die vorsieht, dass bei Verlassen des Arbeitsplatzes keine Unterlagen mit vertraulichen Dokumenten zurückgelassen werden dürfen. Computer müssen gesperrt werden.

9. Der PC als Müllhalde

Einer der Grundsätze des Datenschutzrechts ist die Speicherbegrenzung. Daten sollen nur solange gespeichert werden, wie es für den Zweck der Verarbeitung erforderlich ist. Bestes Beispiel ist das überquellende E-Mail-Postfach.

Dieses sollte regelmäßig geleert werden. Dokumente mit personenbezogenen Daten, die auf der Festplatte gespeichert sind, aber nicht benötgt werden, müssen in den Papierkorb verschoben werden. Achtung: Aufbewahrungsfristen beachten!

10. Datenpannen verschweigen

Jeder Mensch macht mal Fehler. Um Ärger mit den Vorgesetzten zu vermeiden, neigen Mitarbeiter dazu, Datenpannen zu verschweigen. Folge sind Schäden für Betroffene und das Unternehmen.

Sie müssen Mitarbeiter für den Datenschutz sensibilisieren, dessen Bedeutung verdeutlichen und mit gutem Beispiel vorangehen. Schulungen und ständige Thematisierung des Datenschutzes sind hier hilfreich.

Quelle: WELT/ Erdmann Hummel

boldt-IT | Marcus Boldt
An der Marsch 39
29690 Gilten
Germany

Telefon: +49 5071 5215176
Telefax: +49 5071 5215175
Mobil: +49 173 69 100 11
Finanzamt Soltau | Steuer-Nr: 41/105/08516

Bankverbindung:
Hamburger Sparkasse
IBAN: DE19200505501343126874
BIC: HASPDEHHXXX