GDPR (Datenschutzgrundverordnung) – was ist tatsächlich zu tun?

Arthur Braun, M.A

bpv Braun Partners s.r.o.

(+420) 224 490 000
arthur.braun@bpv-bp.com

Der 25. Mai 2018, der erste Tag der Anwendung der neuen EU-Datenschutzgrundverordnung, löst bei vielen Unternehmen grosse Befürchtungen aus.

Zwei Gründe sind dafür verantwortlich: Zum einen der erheblich erhöhte Bussgeldrahmen bis zu 20 Mio EUR oder 4 % des Umsatzes bei Verstössen, vor allem aber, dass Datenschutz bei tschechischen Firmen in der Vergangenheit praktisch nicht relevant war, wohingegen Firmen aus dem deutsche Umfeld schon lange mit Datenschutzbeauftragten, etc. arbeiten. Verstösse wurden bisher in der tschechischen Republik kaum geahndet und Bussgelder waren niedrig. In einigen Monaten gilt aber die direkt anwendbare Verordnung, die auch durch eine lockere Umsatzungspraxis nicht wesentlich gemildert werden kann. Andererseits scheint mir, dass teilweise von Beraterseite unnötig Panik geschürt wird.

Was muss ich als Unternehmer also wirklich tun?

1. Vorab muss sich jeder Unternehmer klarwerden, welche personenbezogenen Daten er verarbeitet, insbesondere, ob es sensitive Daten wie Gesundheitszustand sind, für die besonders strenge Regelungen gelten, oder faktisch nur die Stammdaten seiner Mitarbeiter. Aber Vorsicht, beispielsweise ist auch eine Anmerkung in einer CRM-Datei, dass man einen Kunden nicht zum Steakhaus einladen soll, weil dieser als Hindu kein Rindfleisch isst, solch eine sensitive Information. Und eine Whats-app-Gruppe für datenrelevante Bereiche wie Neueinstellungen zu eröffnen ist sicherlich auch nicht das Idealbild von vorsichtigen Umgang mit Daten. Datenverabeitung kann auch Videoaufzeichnung in der Prokuktionshalle sein! Die nachfolgenden Hinweise gelten auch für die breite Mehrheit der Leser, die nicht solche sensitiven Daten verarbeiten oder dies als Auftragsdatenverarbeiter tun.

2. Wenn ich Kundendaten verarbeite, muss ich möglicherweise den bisherigen Zweck/die Rechtfertigung zur Speicherung und Verarbeitung umformulieren, umso mehr, wenn ich diese Daten weiter gebe. Weitergabe/Spreicherung/Verarbeitung ausserhalb der EU ist unabhängig von der GDPR ein besonderes Problem und sollte unbedingt mit Expertenrat gestaltet werden.

3. Ein Datenschutzbeauftragter muss möglicherweise bestellt werden. Sicherlich nicht, wenn ich ein Produktionsunternehmen bin, das nur Stammdaten der Mitarbeiter verarbeitet, sicherlich schon wenn ich eine Versicherung oder ein Energieunternehmen bin. Selbst wenn dieser bereits besteht, muss ich für ihn möglicherwese einen Arbeitsvertrag vorbereiten.

4. Unabhängig von der Intensität der Datenverarbeitung muss ich prüfen, wer von meinen Mitarbeitern und Dienstleistern Zugang zu diesen Daten hat, ob diese nur zu einem vom Gesetz oder Vertragserfüllung erforderlichen Zweck verarbeitet werden. Auch muss ich selbstverständlich nicht mehr benötigte Daten löschen. Jeder Datenverarbeiter muss geeignete technische und organisatorische Massnahmen zur Minimierung von Datenschutzverletzungen treffen, Art 24/25 GDPR. Eventuell muss ich Verträge mit meinen Dienstleistern nach GDPR aktualisieren.

5. Schliesslich muss ich einen Plan haben, wer und wie das Datenschutzamt im Falle eines leaks, d. h., dass die Daten unberechtigterweise an die Öffentlichkeit gelangen, informiert. Die Verordnung lässt dazu nur 72 Stunden, ohne Rücksicht auf Wochenende oder Feiertage.

Es gibt noch einige weitere Aspekte. Insoweit ist es absolut sinnvoll, einen Check-up der Datenschutzlage im eigenen Unternehmen, ggf. auch durch externe Berater mit zusätzlichen Kenntnissen im Arbeitsrecht, durchzuführen und die entsprechenden Massnahmen einzuleiten. Auch für gut geführte Unternehmen sollten jetzt die Schritte zur Vorbereitung auf die Datenschutzgrundverordnung eingeleitet werden, für Panik ist aber noch kein Anlass.