FDPW
Fachverband Deutscher Präzisions-Werkzeugschleifer

Kompetenz 4.0: Datenschutz:

Braucht mein Unternehmen einen Datenschutzbeauftragten?

Vielen Unternehmern ist bekannt, dass unter bestimmten Voraussetzungen ein Datenschutzbeauftragter benannt werden muss.

Gesetzlich ist das wie folgt geregelt:

- Unternehmen mit mehr als neun Mitarbeitern, die computergestützt mit personenbezogenen Daten arbeiten,
- Unternehmen mit mehr als 20 Mitarbeitern, die ohne Computerunterstützung mit personenbezogenen Daten arbeiten oder
- Unternehmen, die geschäftsmäßig mit personenbezogenen Daten arbeiten

benötigen einen (internen oder externen) Datenschutzbeauftragten.

Häufig weiß die Geschäftsleitung nicht, ob ihr Unternehmen einer dieser Anforderungen tatsächlich unterfällt. Dabei fehlt es an dem notwendigen Fachwissen, wann und wie personenbezogene Daten im täglichen Geschäft überhaupt vorkommen. Dies sind gerade nicht nur Daten von Mitarbeitern, sondern auch entsprechende Angaben von Kunden und Besuchern.

Die EU-Datenschutz-Grundverordnung stärkt den Datenschutz der EU-Bürger, droht Unternehmen aber gleichzeitig mit drakonischen Strafen, falls sie die Richtlinien nicht oder nur unzureichend umsetzen. Um den Anforderungen gerecht zu werden, sollten sie einen Datenschutzbeauftragten bestellen, der Zugriffsrechte penibel verwaltet und die Sicherheit ihres Netzwerks sicherstellt.

Die EU-Datenschutz-Grundverordnung (GDPR) gilt ab **25. Mai 2018** und schafft in Europa einheitliche Datenschutz-Regelungen. Datenschutzverletzungen müssen ab diesem Zeitpunkt innerhalb von **72 Stunden** an die Aufsichtsbehörde gemeldet werden. Außerdem sind die von der Verletzung betroffenen Personen über den Vorfall zu informieren. Die neue Richtlinie ist einerseits für alle Unternehmen

bindend, die einen Sitz in der EU haben, und erstreckt sich andererseits auch auf Firmen weltweit, sofern sie personenbezogene Daten über in der EU ansässige Bürger erheben, verarbeiten und nutzen. Wer sich nicht an die neuen Vorschriften hält, muss mit beträchtlichen Geldstrafen rechnen. Die maximale Geldbuße bei einem schweren Datenschutzvergehen beträgt bis zu **vier Prozent** des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr. Die strikte Einhaltung der GDPR ist daher für Unternehmen aller Branchen überlebenswichtig.

Doch welche Strategien sollten sie verfolgen, um den Anforderungen gerecht zu werden? Drei grundsätzliche Maßnahmen sind bei der Umsetzung der Richtlinien von zentraler Bedeutung:

1. Bestellung eines Datenschutzbeauftragten,
2. die strikte Verwaltung der Zugriffsrechte sowie
3. die wirksame Absicherung des Netzwerkverkehrs.

Das sind die wichtigsten ersten Schritte, um die persönlichen Daten der Kunden wirksam zu schützen, Datenlecks zu verhindern und damit hohe Geldstrafen sowie Image-Verluste zu vermeiden.

Ein Datenschutzbeauftragter gehört zum Pflichtprogramm

Die Bestellung eines Datenschutzbeauftragten ist eine der Voraussetzungen in der GDPR und gilt europaweit. Grundsätzlich steht es dem Unternehmen frei, die Position des betrieblichen Datenschutzbeauftragten intern oder extern zu besetzen. Viele bedienen sich bereits der Möglichkeit, einen externen Datenschutzbeauftragten zu bestellen, um ihre eigenen internen Ressourcen besser zu nutzen und von den Vorteilen des spezifischen Fachwissens eines externen Datenschutzbeauftragten zu profitieren.

Grund: Technologische Neuentwicklungen fordern den Datenschutzbeauftragten zusehends, so dass für ihn eine permanente Weiterbildung in der IT und im juristischen Bereich unerlässlich ist, um den immer komplexeren Fragestellungen gerecht zu werden. Externe Dienstleister wie Systemintegratoren, Systemhäuser oder Reseller haben den wachsenden Bedarf erkannt und bieten mittlerweile die Übernahme dieser Aufgabe als Dienstleistung an. Aber Achtung: Es ist nicht zu empfehlen, aus Sparsamkeit auf einen Datenschutzbeauftragten zu verzichten, da er

der zuständigen **Aufsichtsbehörde gemeldet** werden muss. Eine Unterlassung bleibt daher mit hoher Wahrscheinlichkeit nicht lange unentdeckt.

Muss ich den Datenschutz einhalten, obwohl ich nicht zur Bestellung einen Datenschutzbeauftragten verpflichtet bin?

Weitestgehend unbekannt ist, dass nicht nur Unternehmen, die gesetzlich verpflichtet sind, einen Datenschutzbeauftragten zu bestellen, die datenschutzrechtlichen Gesetze einhalten müssen. So gut wie unbekannt ist, dass unabhängig von den oben genannten Voraussetzungen, wann ein Datenschutzbeauftragter zu bestellen ist, jedes Unternehmen die gesetzlichen Vorgaben für den Datenschutz einhalten muss.

Was passiert, wenn gegen die datenschutzrechtlichen Bestimmungen verstoßen wird?

Es können von dem Unternehmen und der Geschäftsleitung Bußgelder bis zu 300.000 Euro erhoben werden, alleine bis zu 50.000 Euro, wenn ein Datenschutzbeauftragter nicht bestellt wird. Diese Bußen werden sich zukünftig noch verschärfen, wenn **ab Mai 2018** die Vorschriften der europäischen Datenschutzgrundverordnung in Kraft treten. Hier sind Bußgelder in Höhe von vier Prozent des Jahresumsatzes eines Unternehmens vorgesehen.

Weitere Auswirkungen von datenschutzrechtlichen Verstößen:

- Negative Presse-Berichterstattung
- Verlust von Kundenvertrauen
- Ärger mit der Aufsichtsbehörde für Datenschutz
- Keine Aufrechterhaltung von ISO-Zertifizierungen
- Verlust von Aufträgen, wenn Datenschutzbeauftragter nicht benannt werden kann

Wie kann ich mein Unternehmen schützen?

Vor diesen Auswirkungen schützt nur der gesetzeskonforme Umgang mit den persönlichen Daten. Die Bestellung eines Datenschutzbeauftragten, der darüber

wacht, lohnt sich also immer, egal ob die Pflicht für die Bestellung eines Datenschutzbeauftragten besteht oder nicht.

Interner oder externer Datenschutzbeauftragter?

Nur eine fachlich versierte Person ist in der Lage, wirksam über die Einhaltung der datenschutzrechtlichen Bestimmungen zu überwachen.

Ein interner Datenschutzbeauftragter muss kostenintensiv regelmäßig fachlich geschult werden, erledigt seine Aufgabe häufig neben der Hauptaufgabe und erlangt durch seine Bestellung einen erweiterten Kündigungsschutz ähnlich einem Betriebsratsmitglied.
Ein externer Datenschutzbeauftragter ist „Profi“ in seinem Thema. Aktuellstes Wissen kann vorausgesetzt werden. Darüber hinaus haftet der externe Datenschutzbeauftragte für Pflichtverletzungen und muss dem Unternehmen Schäden, die durch die Pflichtverletzung entstehen, ersetzen. Der externe Datenschutzbeauftragte ist neutral gegenüber Abteilungen und Mitarbeitern. Interessenkollisionen sind somit nicht zu befürchten.

Autor:

Pallas GmbH
Jani Nakos
Hermülheimer Straße 8a
D-50321 Brühl

Tel.: 0171 4828422
Tel.: 02232 1896-27
Mail: jani.nakos@pallas.com
Web: www.pallas.com