

# Datenschutz-Quick-Check<sup>1</sup> Selbsttest für Unternehmen

## I. Benötigt Ihr Unternehmen einen Datenschutzbeauftragten?

- Beschäftigt Ihr Unternehmen mindestens zehn Personen ständig mit automatisierter Datenverarbeitung, verfügen also zum Beispiel 10 oder mehr Mitarbeiter über einen PC-Zugang?
- Betreiben Sie besonders datenschutzrelevante Systeme, verarbeiten Sie also etwa sensible personenbezogene Daten, ohne dass Sie hierzu aufgrund von gesetzlichen oder vertraglichen Regelungen ermächtigt sind, speichern Sie Kontaktdaten Dritter zur Weitergabe an andere Unternehmen oder betreiben Sie Markt- oder Meinungsforschung bzw. Scoring-Verfahren?

Sollten Sie **eine der Fragen bejaht** haben: Ihr Unternehmen unterliegt der gesetzlichen Pflicht zur Bestellung eines Datenschutzbeauftragten. Ob und wie Sie dieser Verpflichtung gerecht werden, erfahren Sie in Abschnitt II.

Sollten Sie **beide Fragen verneint** haben, benötigt Ihr Unternehmen voraussichtlich keinen Datenschutzbeauftragten. Dennoch unterliegt Ihr Unternehmen den Datenschutzgesetzen und muss deren Befolgung sicherstellen. Mehr hierzu erfahren Sie in Abschnitt III.

## II. Sollten Sie einen internen oder externen Datenschutzbeauftragten bestellen?

- Verfügt Ihr Unternehmen über ausreichende personelle Ressourcen, um einen internen Datenschutzbeauftragten zu bestellen?
- Verfügt der (designierte) interne Datenschutzbeauftragte über die erforderliche Fachkunde oder kann er diese durch entsprechende Lehrgänge effektiv erwerben?
- Verfügt der (designierte) interne Datenschutzbeauftragte über die erforderlichen Hilfsmittel zur Erfüllung seiner Aufgaben wie einschlägige Literatur, elektronische Tools und vertrauliche IuK-Technik?

<sup>1</sup> Dieser Selbsttest korrespondiert mit komplexen rechtlichen Fragestellungen. Um seine Praktikabilität zu gewährleisten, wurden einige seltene Fallkonstellationen bei der Konzeption außer Acht gelassen. Für die Richtigkeit der Ergebnisse kann daher keine Gewähr übernommen werden.

- Ist der (designierte) interne Datenschutzbeauftragte **nicht** zugleich Geschäftsführer oder Vorstand, Leiter EDV/IT, Personal/HR, Marketing oder Recht bzw. Betriebs-/ Personalrat (Interessenskonflikt)?
- Ergibt eine Kosten-Nutzen-Analyse für Ihr Unternehmen, dass die Bestellung eines internen Datenschutzbeauftragten der Bestellung eines externen Datenschutzbeauftragten vorzuziehen ist?

Sollten Sie **alle Fragen bejahen** können, ist für Ihr Unternehmen die Bestellung eines internen Datenschutzbeauftragten die vorzugswürdige Lösung.

Sollten Sie **nicht alle Fragen bejahen** können, ist für Ihr Unternehmen die Bestellung eines externen Datenschutzbeauftragten anzuraten.

Egal, welche Antworten Sie hier gegeben haben: Fahren Sie mit Abschnitt III fort!

## III. Erfüllt Ihr Unternehmen die datenschutzrechtlichen Kernanforderungen?

- Hat Ihr Unternehmen einen schriftlich bestellten Datenschutzbeauftragten oder ist eine andere Person für die Wahrung des Datenschutzes zuständig, und wird diese Person bei der Einführung/Implementierung datenschutzrelevanter Systeme und Prozesse hinreichend beteiligt?
- Führt Ihr Unternehmen eine „interne Verarbeitungsübersicht“ bzw. das „Verfahrensverzeichnis für jedermann“?
- Sind die Mitarbeiter Ihres Unternehmens mit PC-Zugang auf das Datengeheimnis verpflichtet?
- Führt Ihr Unternehmen eine Dokumentation der Datensicherheitsmaßnahmen (sog. Datensicherheitskonzept)?
- Kann Ihr Unternehmen eine Liste der Zugriffsberechtigungen hinsichtlich der relevanten IT-Systeme vorlegen?
- Kontrolliert Ihr Unternehmen regelmäßig die Datenschutzkonformität der relevanten Systeme und Prozesse (Datenschutzaudit)?
- Soweit externe Dienstleister Zugriffsmöglichkeit auf die Daten Ihres Unternehmens haben, wird die Gewährleistung des Datenschutzes durch dieses Drittunternehmen überwacht?
- Werden Ihre Mitarbeiter im erforderlichen Ausmaß mit den Vorschriften des Datenschutzes ver-

traut gemacht (etwa per Schulungen, Trainingsmaßnahmen oder Informationsmedien)?

Sollten Sie **alle Fragen bejahen** können, erfüllt Ihr Unternehmen die datenschutzrechtlichen Kernanforderungen Anforderungen. Fahren Sie mit Abschnitt IV fort!

Sollten Sie **nicht alle Fragen bejahen** können, verletzt Ihr Unternehmen wesentliche datenschutzrechtliche Pflichten. Berücksichtigen Sie die zusätzlichen Aspekte eines modernen Datenschutzmanagements unter Abschnitt IV und entscheiden sich für eine Handlungsalternative gemäß Abschnitt V.

#### IV. Werden Datenschutzstandards in Ihrem Unternehmen praktisch umgesetzt?

- Bestehen in Ihrem Unternehmen verbindliche Regelungen zum sicheren Umgang mit betrieblicher IuK-Technik?
- Hat Ihr Unternehmen rechtssichere und wirksame Regelungen zur Privatnutzung der betrieblichen IuK-Technik, insbesondere des PC, des Festnetzes, von Mobiltelefonen, des Internet und des Email-Systems getroffen?
- Wissen Ihre Mitarbeiter und Kunden, welche Daten über Sie in Ihrem Unternehmen verarbeitet werden und wer darauf Zugriff hat?
- Soweit Ihr Unternehmen in einen (internationalen) Konzernverbund eingegliedert ist, besteht ein Datenschutzkonzept für konzerninternen Datenfluss?
- Soweit es zu internationalen Datenübermittlungen kommt, ist gewährleistet, dass die Datenempfänger im Ausland ein angemessenes Datenschutzniveau gewährleisten?
- Hat Ihr Unternehmen einen datenschutzkonformen Internetauftritt, der aktuelle, rechtskonforme und abmahnsichere Datenschutzbestimmungen enthält?
- Ist das Haftungs-, Bußgeld- und Sanktionsrisiko für Ihr Unternehmen im Bereich Datenschutz analysiert worden und hat man ggf. entsprechende Vorkehrungen getroffen?
- Soweit Ihr Unternehmen einen Betriebs-/Personalrat hat, wird dieser hinreichend über die Einhaltung des Datenschutzes informiert?

Sollten Sie diese Fragen **bejahen** können, setzt Ihr Unternehmen wesentliche Datenschutzstandards auch in die Praxis um. Entsprechend dürfte das Datenschutzniveau

in Ihrem Unternehmen als ausreichend zu bezeichnen sein. Wir gratulieren Ihrem Unternehmen und insbesondere Ihrem Datenschutzbeauftragten! Abschnitt V ist nicht weiter relevant.

Sollten Sie diese Fragen teilweise **verneinen** müssen, setzt Ihr Unternehmen wesentliche Datenschutzstandards nicht in die Praxis um. Entscheiden Sie sich für eine Handlungsalternative gemäß Abschnitt V.

#### V. Handlungsalternativen

Sofern Ihr Unternehmen die erforderlichen Maßnahmen zum Datenschutz bisher nicht eingeleitet hat, ergeben sich folgende Handlungsalternativen:

##### 1. Datenschutzbeauftragter ist bestellt

- Sie konfrontieren den Datenschutzbeauftragten Ihres Unternehmens mit den Ergebnissen dieses Selbsttests und bitten um Stellungnahme.
- Sie fordern Ihren Datenschutzbeauftragten dazu auf, die erforderlichen Maßnahmen zum Datenschutz einzuleiten.
- Sie bieten Ihrem Datenschutzbeauftragten an, sich durch fachkundige Experten auf dem Gebiet des Datenschutzes unterstützen zu lassen.

##### 2. Bisher kein Datenschutzbeauftragter bestellt

- Sie empfehlen Ihrem Unternehmen die Beauftragung eines Mitarbeiters mit der Umsetzung der erforderlichen Datenschutzmaßnahmen oder die Bestellung eines internen Datenschutzbeauftragten unter Berücksichtigung der Abschnitte I und II.
- Sie bestellen einen externen Datenschutzbeauftragten und beauftragen ihn mit der Umsetzung der erforderlichen Maßnahmen.