RABER & COLL.

Rechtsanwälte

Gerhart-Hauptmann-Straße 6
99096 Erfurt
Telefon: (0361) 43 05 63 7

E-Mail: recht@raberundcoll.de
Telefax: (0361) 43 05 63 99

www.raberundcoll.de

INFO-Post

6/2013

Die anlasslose Kontrolle des Landesbeauftragen für Datenschutz gem. § 38 BDSG

Verstärkt erhalten Unternehmen in Thüringen Post vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit.

Inhalt des Schreibens: Ankündigung einer Kontrolle des Unternehmens im Hinblick auf die Einhaltung der Regelungen des Bundesdatenschutzgesetzes (BDSG).

Diese INFO-Post soll Ihnen einen Einblick geben, was geprüft wird und was Sie im Vorfeld unternehmen können, um ein mögliches Bußgeld zu vermeiden.

QUALITÄT DURCH FORTBILDUNG
Fortbildungszertifikat der Bundesrechtsanwaltskammer

I. Das Kontrollrecht des Landesbeauftragten für Datenschutz

Gem. § 38 Abs. 4 Bundesdatenschutzgesetz (BDSG) ist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) berechtigt, eine Durchsuchung durchzuführen. Zweck der Durchsuchung ist es festzustellen, inwiefern die Datenschutzbestimmungen eingehalten werden.

Dem TLfDI steht folgendes Instrumentarium zur Verfügung:

- Er darf geschäftliche Unterlagen einsehen.
- Er darf die Übersicht nach § 4 g Abs. 2 Satz 1 BDSG einsehen.
- Er darf die gespeicherten personenbezogenen Daten einsehen
- Er darf die Datenverarbeitungsprogramme einsehen.

II. Inhalt der Kontrolle

Folgende Themenbereiche des Datenschutzrechts werden kontrolliert:

1. Rechtsgrundlagen der Datenerhebung

Jede Datennutzung bedarf einer Rechtfertigung im Sinne einer Rechtsgrundlage. Auf welche Rechtsgrundlagen wird der Umgang mit personenbezogenen Daten in Ihrem Unternehmen gestützt? Rechtsgrundlagen können sein:

- Eine gesetzliche Vorschrift. Zum Beispiel:

> § 32 Abs. 1 BDSG
> „*Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist*."

- Eine wirksame Einwilligung des Betroffenen gem. § 4 Abs. BDSG.

Sollten also Daten der Mitarbeiter über den Zweck der Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses hinaus gespeichert werden, sollte eine wirksame Einwilligung vorliegen.

2. Der Datenschutzbeauftragte

Gibt es in Ihrem Unternehmen einen Datenschutzbeauftragten? Die Pflicht einen eigenen Datenschutzbeauftragten zu bestellen besteht, sobald mehr als neun Personen im Unternehmen ständig mit der automatisierten Verarbeitung personenbezogener Daten zu tun haben, § 4 f BDSG. Der Betrieb muss spätestens einen Monat nach Aufnahme seiner Tätigkeit einen Datenschutzbeauftragten bestellen, § 4 Abs. 1 Satz 2 BDSG. Bei Nichtbestellung oder verspäteter Bestellung liegt eine Ordnungswidrigkeit vor und kann mit einem Bußgeld von bis zu 50.000 € geahndet werden, § 43 Abs. 3 BDSG.

a. Aufgaben des Datenschutzbeauftragten:

- Allgemeine Beratung der Geschäftsführung
- Mitarbeiterschulung
- Regelmäßige Kontrolle der technischen bzw. organisatorischen Umsetzung des Datenschutzes im Unternehmen
- Ansprechpartner für Mitarbeiter und Betroffene
- Durchführung der Vorabkontrolle
- Führen des Verfahrensverzeichnisses
- Erstellung des Datenschutzkonzeptes
- Jährliche Überprüfung des Datenschutzkonzeptes auf Aktualität

b. Anforderungen an den Datenschutzbeauftragten

aa. Fachkunde im Datenschutzrecht

Über die folgenden technischen bzw. organisatorischen Kenntnisse muss der Beauftragte für den Datenschutz verfügen:

- Grundlegende Kenntnisse der Persönlichkeitsrechte der Betroffenen und Mitarbeiter
- umfassende Kenntnisse der Regelungen des BDSG
- umfassendes Wissen bzgl. datenschutzrechtlicher und technischer Vorschriften, der Datenschutzprinzipien und der Datensicherheitsanforderungen. Zudem muss die Geeignetheit von technischen und organisatorischen Maßnahmen beurteilt werden können.

bb. Branchenspezifische Kenntnisse

Die Anforderungen variieren je nach Branche, IT-Infrastruktur, Größe der Organisation und der Sensibilität der Daten:

- Kenntnis der für das Unternehmen relevanten Datenschutznormen
- Fachwissen in der Informationstechnologie und der Datensicherheit
- Betriebswirtschaftliches Sachverständnis
- Wissen um die Strukturen und Abläufe im Unternehmen
- Praktisches Datenschutzmanagement

cc. Rahmenanforderungen

Gewisse Rahmenbedingungen muss der Arbeitgeber gewährleisten:

- Der Datenschutzbeauftragte darf in keinen Interessenkonflikt geraten. So darf er sich nicht selbst überwachen. So scheiden Angehörige der Geschäftsleitung grundsätzlich aus.
- Dem Datenschutzbeauftragten ist ein Recht zur Verschwiegenheit bezüglich sensibler Daten gegenüber der Unternehmensführung zuzugestehen.
- Dem Datenschutzbeauftragen sind die erforderlichen Zutritts- und Einsichtsrechte einzuräumen.
- Die Weiterbildung des Datenschutzbeauftragten ist zu gewährleisten.
- Dem internen Datenschutzbeauftragten ist die notwendige Zeit zur Erfüllung seiner Pflichten einzuräumen.

c. Interner oder externer Datenschutzbeauftragter?

Man kann einen internen Datenschutzbeauftragten bestellen oder einen externen Datenschutzbeauftragten beauftragen.

aa. Vorteile des internen Datenschutzbeauftragten

- Er ist in die tägliche Kommunikation eingebunden.
- Er kennt das Unternehmen, die Mitarbeiter sowie die allgemeinen Abläufe.
- Da kein externer Dienstleister beauftragt wird, fallen keine unmittelbaren Kosten an.

bb. Nachteile des internen Datenschutzbeauftragten

- Er genießt Kündigungsschutz.
- Oft sind die vorhandenen Mitarbeiter in datenschutzrechtlicher Hinsicht nicht hinreichend qualifiziert und Erfüllen so das Kriterium der Fachkunde nicht.
- Defizite in der fachlichen Eignung und das Phänomen der „Betriebsblindheit“ können zu nicht sachgerechten, ineffizienten Maßnahmen führen.
- Die Kosten sind schwer zu beziffern, so zum Beispiel im Hinblick auf die zeitliche Inanspruchnahme oder die Weiterbildungskosten.

cc. des externen Datenschutzbeauftragten

- Er kennt eine Vielzahl von Datenschutzkonzepten verschiedener Unternehmen und überblickt den Markt.
- Dadurch arbeitet er schneller und kann auf bestehende Unterlagen zurückgreifen.
- Es entsteht kein internes Konkurrenzverhalten bezüglich des Datenschutzbeauftragten.
- Erhöhte Akzeptanz durch den Betriebsrat.

dd. Nachteile externer DSB

- Unmittelbare Kosten durch die Beauftragung.
- Er ist nicht in die Unternehmenskommunikation eingebunden, somit immer „fremd“.
- Mangelndes Vertrauen der Mitarbeiter in einen externen Berater.
- Oft fehlt die nötige Branchenkenntnis.

d. Die Abberufung

Beachtet werden sollte unbedingt, dass die Aufsichtsbehörde die Abberufung des Datenschutzbeauftragten verlangen kann, falls er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt. Dies kann in der Folge zur Verhängung eines Bußgelds führen.

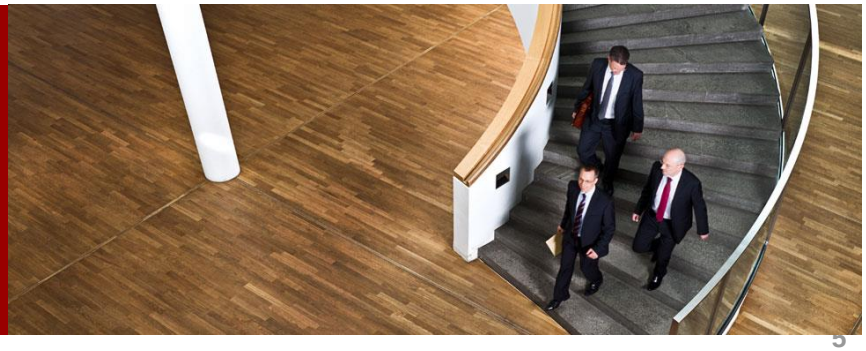
3. Das Verfahrensverzeichnis

Gem. § 4 g Abs. 2 BDSG müssen Sie ein Verfahrensverzeichnis erstellen. Dies soll transparent darstellen, wie im Unternehmen personenbezogene Daten verarbeitet werden.

Dazu werden folgende Punkte dokumentiert:

- Welche personenbezogenen Daten werden
- unter Verwendung welcher automatisierter Verfahren
- auf welche Weise verarbeitet und
- welche Datenschutzmaßnahmen wurden umgesetzt, um diese Daten zu schützen?

Zudem erhöht das Verfahrensverzeichnis die Auskunftsfähigkeit gegenüber Mitarbeitern, Kunden und den Behörden und schafft Vertrauen.



4. Das Datengeheimnis

Das Datengeheimnis nach § 5 BDSG muss von jeder Person, die mit der Datenverarbeitung beschäftigt sind, beachtet werden. Dies muss durch eine rechtlich einwandfreie Verpflichtungserklärung dokumentiert werden.

> *§ 5 BDSG*
> *„Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.“*

5. Outsourcing

Soweit Ihr Unternehmen Daten an externe Dienstleister wie z. B. Unternehmensberater, Steuerberater, Büro-Software, Webhoster, Cloud-Dienste etc. weitergibt, müssen bei der Auswahl des externen Dienstleisters und während der Vertragslaufzeit gewisse datenschutzrechtliche Kriterien erfüllt sein und kontrolliert werden.

6. Videoüberwachung

Gesetzlich geregelt ist die Videoüberwachung in § 6b BDSG. Falls eine Videoüberwachung stattfindet, werden folgende Fragestellungen relevant sein:

- Für welche Zwecke erfolgt die Videoüberwachung?
- Gibt es schriftliche Festlegungen zum Zweck?
- Mit welchen Mitteln erfolgt die Überwachung?
- Nur Beobachtung oder auch Aufzeichnung?
- Wer hat Zugriff auf die Daten?
- Speicherung für welchen Zeitraum?
- Wann erfolgt eine Löschung der Daten?

7. Private Nutzung betrieblicher Kommunikationsmittel

Die private Nutzung betrieblicher Kommunikationsmittel ist datenschutzrechtlich problematisch. Regelungen in Arbeitsverträgen oder entsprechende Zusatzvereinbarungen mit den Arbeitnehmern schaffen hier Klarheit.

8. Sperrung / Löschung nicht mehr erforderlicher Daten

Hierzu muss es ebenfalls klare Handlungsanweisungen geben.

9. Technische / organisatorische Maßnahmen

Existieren hinreichende technische bzw. organisatorische Maßnahmen im Unternehmen, um die Umsetzung des BDSG zu gewährleisten?

> *„§ 9 BDSG*
> *Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."*

Beispiele:

- Werden alte Datenträger mit personenbezogenen Daten datenschutzgerecht gelöscht?
- Wird sensibles Altpapier datenschutzgerecht entsorgt?
- Werden E-Mails mit personenbezogenen Daten verschlüsselt?

10. Notfallplan für den Notfall nach § 42 a BDSG

Existiert ein Notfallplan für den Fall eines Datenlecks?

III. Aussageverweigerungsrecht

Beachten Sie bitte, dass Sie gem. § 38 Abs. 3 BDSG ein Aussageverweigerungsrecht haben, sobald Sie sich während der Kontrolle aufgrund einer Frage einer strafrechtlichen Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten ausgesetzt sehen.

IV. Fazit

Wie Sie bemerkt haben, stellt der Gesetzgeber umfangreiche Anforderungen an Ihr Unternehmen. Die Erfüllung dieser Anforderungen ist in rechtlicher wie auch in tatsächlicher Hinsicht gerade für vielbeschäftigte Unternehmer, die nicht im Datenschutzrecht bewandert sind, eine komplexe Herausforderung, welche Risiken in Form einen Bußgeldes oder eines Vertrauensverlustes der Mitarbeiter oder Kunden birgt.

Bei der Bewältigung dieser Herausforderung stehen wir Ihnen gern tatkräftig mit unserem Fachwissen sowie mit praktischen Lösungsvorschlägen, Handlungsanleitungen und Formularvorlagen zur Verfügung.

Rechtsanwalt Martin Krah