www.datenschutz-praxis.de

WEKA

Datenschutz PRAXIS

RECHTSSICHER | VOLLSTÄNDIG | DAUERHAFT

Ausgabe Februar 2013 | 12 € zzgl. MwSt.

Quelle: Thinkstock

Internes Audit durch den DSB

Compliance-Audit in der Personalabteilung

Die Sicherheit der Personaldaten hat naturgemäß einen hohen Stellenwert im Unternehmen. Verständnis für notwendige Datenschutzmaßnahmen ist seitens der Geschäftsleitung sowie der Mitarbeiter üblicherweise vorhanden. Doch haben Sie schon einmal nach einiger Zeit die Umsetzung und Einhaltung der Datenschutzvorgaben in der Personalabteilung überprüft?

Ein Compliance-Audit ist die Überprüfung der Übereinstimmung von Realität und festgelegtem Regelwerk. Es geht also um die Kontrolle, ob definierte Prozesse, Anforderungen und Richtlinien eingehalten werden.

Üblicherweise führen speziell geschulte Auditoren die Prüfungen durch. Mit entsprechender Vorbereitung gelingt dies jedoch auch Ihnen als Datenschutzbeauftragtem.

Ziele des Audits

Im Bereich der Personalverwaltung haben Sie sicherlich bereits Anregungen und Datenschutzhinweise für eine gesetzeskonforme Datenverarbeitung ausgearbeitet. Die vorgeschlagenen Maßnahmen gilt es ab und an auf ihre Wirksamkeit und vor allem auf ihre Umsetzung in die tägliche Praxis zu überprüfen.

Des Weiteren ist ein regelmäßiger Abgleich mit der Dokumentation Ihrer Verfahrensübersichten und Anwendungsbeschreibungen durchzuführen. Nur so lässt sich deren Aktualität sicherstellen.

Gibt es mittlerweile neue Verfahren oder Schwachstellen?

Ein Audit sollte neben der „profanen“ Überprüfung der ursprünglichen Ziele anhand Ihrer Daten-

Fortsetzung auf Seite 8

ISSN-Nr. 1614-6867

Fortsetzung von Seite 1

schutzdokumentation auch dem Zweck zugutekommen, neue Verarbeitungsschritte im Umgang mit Personaldaten festzustellen. Eventuell spüren Sie im Rahmen Ihres Audits auch weiteren Verbesserungsbedarf beim Schutz von personenbezogenen Daten auf.

Ein Audit sollte periodisch stattfinden

Grundsätzlich ist ein Audit keine einmalige Angelegenheit. Sinnvoll ist z.B. ein maximales Intervall von zwei Jahren für die periodische Nachkontrolle. Der Aufwand für die Ausarbeitung eines detaillierten Auditplans ist also keinesfalls umsonst.

Eine gute Vorbereitung ist das A und O

Gerade für Datenschutzbeauftragte, die mit den Feinheiten eines durch Profis durchgeführten Audis nicht vertraut sind, empfiehlt sich eine strukturierte Vorbereitung. Ihre Vorteile sind Ihre Qualifikation, Ihr besonderes Wissen zum Thema Datenschutz sowie Ihre hoffentlich vorhandene Datenschutzdokumentation.

Umfangreiches Prüfungsumfeld

Insbesondere in der Personalabteilung bzw. im Human-Resources-Bereich ist eine Fülle von Themen zu prüfen, die den Datenschutz berühren. Je nach Unternehmen fallen darunter auf jeden Fall die klassischen Bereiche wie

- Bewerbungs-/Einstellungsverfahren,
- Personalinformationssysteme (PIM),
- Anwesenheits-/Zeitverwaltung sowie
- Führung der Personalakten.

Relevante Spezialthemen

Nicht zu vergessen im Rahmen eines Audits sind Spezialthemen. Möglicherweise kommen sie in Ihrem Unternehmensumfeld nicht oder nicht alle zum Tragen, jedoch sollten Sie zumindest die Thematik bei den Verantwortlichen ansprechen. Als Beispiele wären hier zu nennen:

- Mitarbeitervergünstigungen (namentlich Zusatzversicherungen, Kfz-Nutzung oder dergleichen)
- betriebliches Eingliederungsmanagement
- Überwachungsmaßnahmen z.B. durch Videoanlagen
- Sarbanes Oxley Act (SOX) bzw. EuroSOX
- Datenscreening zur Korruptionsbekämpfung
- EG-Antiterrorismusverordnung

Die Rechtmäßigkeit der Datenerhebung und -verarbeitung muss auch in diesen speziellen Anwendungsfällen geprüft und dokumentiert werden.

Datenzyklen dienen als Auditleitfaden

Für ein Compliance-Audit in der Personalabteilung ist es sinnvoll, die Mitarbeiterdaten in verschiedene Datenzyklen einzuteilen:

- Es beginnt bei Personaldaten beispielsweise mit dem Bewerberverfahren,
- geht über Einstellung und Einarbeitung in die
- Arbeitnehmerverwaltung bis hin zum
- Ausscheiden eines Mitarbeiters und
- endet mit den Specials.

Erfahrungsgemäß stehen in jedem Mitarbeiterzyklus andere Beschäftigtendaten im Vordergrund. Oftmals ist zudem der Kreis der Verantwortlichen, die mit der Aufgabenstellung betraut sind, unterschiedlich – zumindest in größeren Unternehmen.

Datenschutzdokumentation und Audit-Kernfragen

Die nächste Stufe ist nun die Ausarbeitung von Kernfragen für die verschiedenen Bereiche. Orientieren Sie sich dabei an Ihrer Datenschutzdokumentation und Ihren Verfahrensdefinitionen. Das nebenstehende Muster „Compliance-Audit zum Bewerberverfahren“ stellt einen passenden Fragenkatalog als Beispiel für Sie zusammen.

Bewertungsmaßstab

Ein Audit lebt von Prüfungsfragen, Auditbeobachtungen und deren Bewertungen. In der Spalte „Wertung“ aus unserem Beispiel können Sie beispielsweise vermerken:

A0 = nicht relevant
A1 = Erwartung erfüllt
A2 = Vorgaben teilweise erfüllt
A3 = Nachbesserung notwendig
A4 = nicht erfüllt

Je nach Beurteilung sind entsprechende Nacharbeiten notwendig, um Ihre Forderungen an einen adäquaten Datenschutz zu erfüllen.

Auditbeobachtung eintragen

In die Spalte „Anmerkung“ können Sie weitere Auditbeobachtungen oder zusätzliche Informationen eintragen. Bei der Beispielfrage „Gibt es Regelungen zur vollständigen Rücksendung der Unterlagen bei abgelehnten Bewerbern?“ könnte der Befragte z.B. darauf hinweisen, dass der Betriebsrat eine Kopie des Lebenslaufs zurückbehält. Diese Information ist zwingend festzuhalten und wäre mit den entsprechenden Stellen abzuklären.

Idealerweise sind die Punkte „erledigt“

Die letzte Spalte im Musteraudit erklärt sich von selbst. Haken dran – sofern kein weiterer Handlungsbedarf besteht und das Thema entsprechend den definierten Vorgaben umgesetzt wird. Muss das Kästchen leer bleiben, besteht nach wie vor Aktionsbedarf für den Datenschutzbeauftragten.

Organisatorische Anforderungen sind damit erfüllt

Die organisatorischen Anforderungen wären damit nun erfüllt. Ob Sie Ihren

Audit-Katalog in einer gängigen Office-Anwendung wie Word oder Excel aufbauen oder ein professionelles Tool wie das kostenlose Produkt VERINICE (*www.verinice.org/*) einsetzen, bleibt Ihnen überlassen. Natürlich bietet sich für ein umfangreiches Audit auch ein fertiges Produkt aus dem WEKA-Verlag an wie z.B. „Personaldaten datenschutzgerecht verwalten“ (*http://shop.weka.de/personaldaten-datenschutzgerecht-verwalten*).

Rechnen Sie mit Nacharbeiten

Ein Compliance-Audit soll die definierten Datenschutzregeln kontrollieren, die Einhaltung der internen Verpflichtungen sicherstellen und ihre Wirksamkeit im Unternehmen festhalten. Zielsetzung ist, Compliance-Abweichungen frühzeitig zu erkennen oder eventuelle Verstöße, aber auch geänderte Verfahrensschritte aufzudecken und zu dokumentieren.

Rechnen Sie damit, dass nach einem solchen Audit meist noch Nacharbeiten erforderlich sind. Denn in den seltensten Fällen stimmen die Erhebungen aus einem Audit hundertprozentig mit Ihren Datenschutzdokumentationen und Leitlinien überein.

Hermann Keck

Hermann Keck ist externer Datenschutzbeauftragter (*www.keck-dsb.de*).

Prüfungsfrage	Wertung	Anmerkung	erledigt
Wird der Grundsatz einer diskriminierungsfreien Stellenausschreibung nach AGG beachtet?			☐
Werden Stellenausschreibungen in Zeitungen/Zeitschriften oder im Internet veröffentlicht (Muster vorlegen lassen)?			☐
Abgleich der internen Verfahrensübersicht „Bewerbungsverfahren“ mit aktueller Handhabung			☐
Gibt es Regelungen zur vollständigen Rücksendung der Unterlagen bei abgelehnten Bewerbern?			☐
Wird die Informationspflicht nach § 33 Abs. 1 BDSG beim Rückbehalt von Bewerbungskopien beachtet?			☐
Wird eine Anreicherung von Bewerbungsdaten über Internetplattformen (XING, LinkedIn, Facebook usw.) durchgeführt? Rechtmäßigkeit als „öffentliches Verzeichnis“ prüfen!			☐
Enthält der Interview-Leitfaden für Vorstellungsgespräche nur zulässige Fragen (aktuellen Leitfaden vorlegen lassen)?			☐
Werden gesondert Daten zur Beweislastführung nach § 22 AGG aus Bewerbungsunterlagen und/oder Vorstellungsgesprächen gespeichert?			☐
Ist die datenschutzkonforme Löschung von Bewerbungsdaten, insbesondere auch der elektronischen Daten, nach Ablauf des Einstellungsverfahrens sichergestellt?			☐
Ist der Kreis von zugriffsberechtigten Personen definiert?			☐

Auditor _____ Datum _____

Befragter _____ Version 1.x

Muster für ein Compliance-Audit „Bewerberverfahren“. Das Muster finden Sie zum kostenlosen Download unter www.datenschutz-praxis.de/fachwissen/vorlagen/muster.