# Umsetzung der DSGVO im HR-Management

Arbeitgeber werden in allen drei Stadien des Beschäftigungsverhältnisses (Begründung, Durchführung und Beendigung) nicht nur mit arbeitsrechtlichen, sondern auch mit datenschutzrechtlichen Fragestellungen konfrontiert. Ungeachtet des Inhalts der jeweiligen (zukünftigen) Arbeitsleistung und unabhängig davon in welcher Phase der Beschäftigung der Arbeitgeber personenbezogene Daten erhebt und verarbeitet, ist sicherzustellen, dass die datenschutzrechtlichen Vorgaben eingehalten werden. Moderner Datenschutz im Betrieb stellt ein Zusammenspiel aus Personalabteilung, Rechtsabteilung, IT und Compliance-Organisation eines Unternehmens dar. Inhaltlich geht es letztlich um Qualitäts-Management (QM). Um alle betrieblichen Abläufe in Einklang mit den gesetzlichen Vorgaben zu bringen, müssen auch die übrigen Fachabteilungen von Beginn an sehr eng mit den Datenschutzexperten (egal ob interne oder externe) zusammenarbeiten.

Dieses Praxishandbuch soll Ihnen, als Arbeitgeber, als praktisches Nachschlagewerk bei diversen Fragestellungen rund um den Datenschutz in Bezug auf Arbeitnehmerdaten dienen. Neben zehn Organisationsschritten zu einer DSGVO-konformen Handhabung der personenbezogenen Daten finden Sie Antworten auf 100 häufig gestellte datenschutzrechtliche Fragen in der Personalabteilung.

Die folgende Arbeitsanleitung hilft, checklistartig allen HR-Verantwortlichen in

**10 Organisationsschritten**

vorhandene Mängel aufzudecken, zu beseitigen und positiv entsprechende Maßnahmen zu ergreifen, um das neue Datenschutzregime effektiv einhalten und letztlich auch zu einem besseren Verständnis des eigenen Betriebs nutzen zu können.

## Schritt 1: Überprüfen Sie vor jeder Verarbeitung von personenbezogenen Daten die Rechtmäßigkeit und sorgen Sie für ausreichende Datenschutzmanagementsysteme.



Arbeiten Sie mit einer strukturierten Datenbank, die selektives Löschen ermöglicht. Zu viele Daten befinden sich nach wie vor in unstrukturierten elektronischen Informationen wie E-Mails, SMS, WhatsApp oder auch Fo-

tos. Optimal ist der Einsatz einer strukturierten Datenbank, in der Unternehmen die exponentiell steigende Datenmenge auch zukünftig im Griff behalten. Stellen Sie dabei sicher, dass für jede Datenverarbeitung eine erforderliche Erlaubnis vorliegt und diese nur im notwendigen Maß stattfindet. Greifen Sie für Datenverarbeitungen im Rahmen der Beschäftigtenverhältnisse *nicht* primär auf die Einwilligungen der Mitarbeiter zurück, denn in den meisten Fällen sind diese weder hilfreich noch erforderlich, weil die Rechtmäßigkeit ohnehin aufgrund des Dienstverhältnisses oder einer gesetzlichen Grundlage gegeben ist. Zur Bedeutung der Einwilligung im Beschäftigtendatenschutz siehe Fragen 55 bis 58.

**Schritt 2: Beachten Sie die Transparenz- und Dokumentationspflichten im Hinblick auf HR-Prozesse.**

Neben der Einhaltung der datenschutzrechtlichen Vorgaben, müssen Sie diese auch nachweisen können (Rechenschaft). Beachten Sie Ausmaß und Notwendigkeit der Datenverarbeitung. Jedes „Plus" an personenbezogenen Daten stellt ein Risiko für Unternehmen dar. Es dürfen voreingestellt nur die Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck auch wirklich erforderlich sind.

Dokumentieren Sie daher Ihre Umsetzungen von technischen und organisatorischen Maßnahmen, Einbindungen des Datenschutzbeauftragten und Betriebsrates, vorgenommene Datenschutzschulungen, Verpflichtungen zum Datengeheimnis, Meldungen von Datenschutzverstößen sowie Prozesse zur Wahrnehmung von Betroffenenrechten.

Informieren Sie auch Ihre Beschäftigten sowie Bewerber, zu welchen Zwecken die personenbezogenen Daten erhoben werden, wer Datenschutzbeauftragter ist, an welche Empfänger die Daten gehen und welche Betroffenenrechte den Arbeitnehmern nach der DSGVO zustehen.

**Schritt 3: Trennen Sie – auch gedanklich – bei der datenschutzkonformen Organisation ihrer HR-Prozesse ihre Mitarbeiterdaten (= Personaldaten) vom Umgang der Mitarbeiter mit ihren Kundendaten (Klienten-/Patienten-/Mandantendaten).**

Fassen Sie Ihre Datenverarbeitung als „Datenbuchhaltung" auf. Weisen Sie den unterschiedlichen Verarbeitungstätigkeiten auch getrennte „Konten" zu.

Die Unterscheidung zwischen kundennahen Themen des Datenschutzes und rein auf die (interne) Personalverarbeitung bezogene Bereiche, schafft

Klarheit und Übersichtlichkeit. Zu den kundennahen Themen gehören ua die Betroffenenrechte, erweiterte Informationspflichten, das Recht auf Datenänderung und Datenlöschung, das Recht auf Datenportierung (Art 19 DSGVO), der Umgang mit Verbandsanfragen/Verbandsklagen sowie das Recht auf Schadenersatz (materiell/immateriell). Diese Themen spielen im Beschäftigtenverhältnis eher eine untergeordnete Rolle, da die Personaldaten weitestgehend auf gesetzlicher Grundlage oder in Erfüllung des Dienstvertrages verarbeitet werden. Erstellen Sie daher eine „Landkarte der Personalprozesse" und vergeben Sie Teilprozesse und Aufgaben mit Bezug auf Datenschutz. Der Klassifizierung von Personalprozessen folgt die Identifikation von Beschäftigungsdaten und die systematische Erfassung letztlich aller Personalaktendaten.

### Schritt 4: Verpflichten Sie Ihre Mitarbeiter durch geeignete Erklärungen zur Einhaltung des Datengeheimnisses nach § 6 DSG 2018.

Beziehen Sie alle Mitarbeiter aktiv in den Datenschutz ein. Auf Information und Beteiligung folgen Engagement und Commitment. Neben zahlreichen Betriebs- und Geschäftsgeheimnissen kommt der Arbeitnehmer bei der Ausübung seiner Tätigkeit im Betrieb mit zahlreichen personenbezogenen Daten von Kunden sowie Mitarbeitern in Berührung.

Sie haben den Arbeitnehmer daher nach § 6 DSG 2018 zu verpflichten, sämtliche Vorgänge, Geschäftsgeschehnisse und Daten gegenüber Dritten zu wahren. Sie finden dazu ein passendes MUSTER I im Anhang dieses Buches. Diese Geheimhaltungsverpflichtung gilt sowohl während des aufrechten, als auch nach Beendigung des Arbeitsverhältnisses. Verpflichten Sie daher jeden einzelnen Arbeitnehmer bei Aufnahme der Tätigkeit zur Beachtung des gesetzlichen Verbots unbefugter Datenerhebung und -verwendung (siehe Fragen 52 bis 54 zum Datengeheimnis).

### Schritt 5: Führen Sie regelmäßig Datenschutzschulungen durch und bereiten Sie Ihre Mitarbeiter auf mögliche Datenpannen vor.

Verlassen Sie sich nicht auf die ISO/IEC 27001 Zertifizierung. Die ISO/IEC 27001 Zertifizierung reicht als Nachweis eines angemessenen Schutzes gegen unbefugte Zugriffe auf personenbezogene Daten alleine nicht aus. Es liegt in Ihrer Verantwortung, den Mitarbeitern das Bewusstsein für die wichtigsten DSGVO-Anforderungen zu schaffen. Führen Sie daher regelmäßig Datenschutzschulungsmaßnahmen durch.

Reagieren Sie schnell bei einer Datenschutzverletzung: Die DSGVO beinhaltet eine klare Vorgabe bei Datenpannen (*data breach*), binnen 72 Stunden nach Erkennen, bei der zuständigen Aufsichtsbehörde eine Meldung zu machen. Daher sollten Sie schon vorbereitend konkrete Abläufe fixieren und Übungen durchführen, um Ihre Mitarbeiter auf mögliche Datenpannen und Anfragen von betroffenen Personen vorzubereiten. So stellen Sie sicher, dass Mitarbeiter sich ihrer Verantwortung in Bezug auf den Schutz und der Erkennung von Schutzverletzungen personenbezogener Daten bewusst werden. Erstellen Sie Merkblätter sowie Leitlinien im Umgang mit personenbezogenen Daten und führen Sie in Ihrem Unternehmen eine Datenschutzrichtlinie ein. Sie finden dazu ein passendes MUSTER V im Anhang dieses Buches.

### 6 Schritt 6: Erstellen Sie das Verarbeitungsverzeichnis (VVZ) Ihres Unternehmens mit großer Sorgfalt.

Es bildet das Rückgrat all ihrer Dokumentationsbemühungen, gewissermaßen den „Kontenrahmen Ihrer Datenbuchhaltung", denn darin sind sämtliche Verarbeitungstätigkeiten in der HR nach Datenarten, Herkunft, Empfängerkreis, Zweck und Rechtsgrundlage geordnet erfasst. Diese „Datenbuchhaltung" fordert die Datenschutzbehörde bei jeder Überprüfung Ihres Betriebes zuerst an.

Prüfen Sie, ob Ihr Unternehmen neben der Verantwortlichenfunktion auch Aufgaben als Auftragsverarbeiter wahrnimmt. Diesfalls sind Sie verpflichtet zwei (unterschiedlich aufgebaute) Verarbeitungsverzeichnisse zu führen. Sie finden ein passendes MUSTER IV für ein Auftragsverarbeiter-VVZ im Anhang des Buches.

### 7 Schritt 7: Halten Sie das Verarbeitungsverzeichnis (VVZ) Ihres Unternehmens stets aktuell.

Wenn sich Prozesse in Ihrem Betrieb verändern oder neue Geschäftsfelder hinzukommen, passen Sie das Verarbeitungsverzeichnis an, gegebenenfalls erweitern Sie es. Der Grundsatz der Datenaktualität ist immer einzuhalten. Verfügen Sie stets über ein aktuelles und inhaltlich richtiges Verarbeitungsverzeichnis. Unternehmen benötigen ein flexibles und sicheres Verzeichnis, das sämtliche Verarbeitungsvorgänge im Umgang mit personenbezogenen Daten dokumentiert. Excel kann hier nur als kurzfristige Notlösung dienen, denn die Dokumentation ist sehr textlastig. Für den langfristigen Gebrauch empfehlen sich daher bei bis zu ca 25 Verarbeitungstätigkeiten Textverarbeitungsprogramme und darüber hinaus professionelle Datenschutz-Doku-