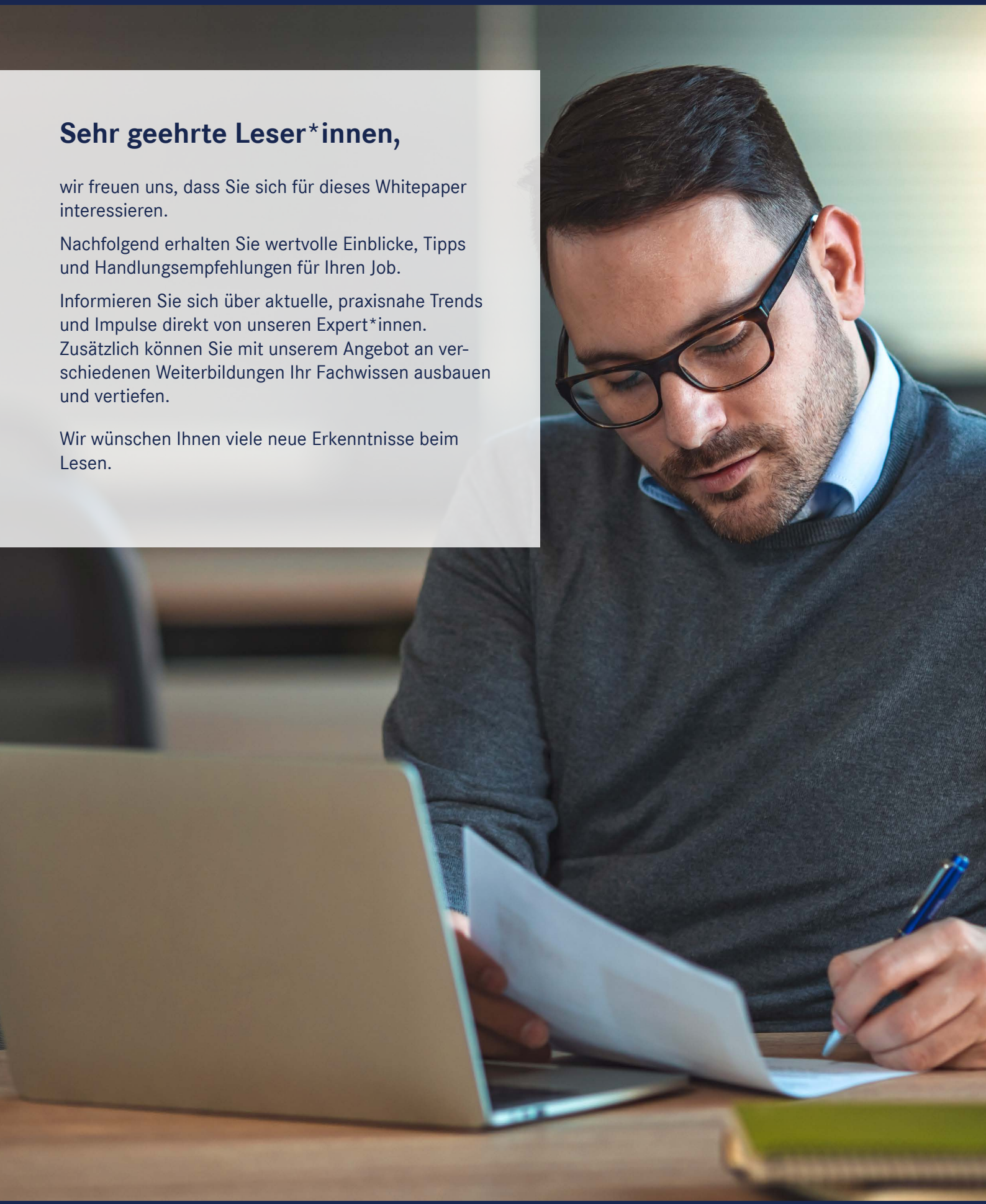
FORUM

Datenschutz in der Personalarbeit – Fundierte Compliance für HR-Verantwortliche

DSGVO im HR-Bereich: Datenminimierung, Integrität und Schutz sensibler Personaldaten.



Sehr geehrte Leser*innen,

wir freuen uns, dass Sie sich für dieses Whitepaper interessieren.

Nachfolgend erhalten Sie wertvolle Einblicke, Tipps und Handlungsempfehlungen für Ihren Job.

Informieren Sie sich über aktuelle, praxisnahe Trends und Impulse direkt von unseren Expert*innen. Zusätzlich können Sie mit unserem Angebot an verschiedenen Weiterbildungen Ihr Fachwissen ausbauen und vertiefen.

Wir wünschen Ihnen viele neue Erkenntnisse beim Lesen.

Dieses Whitepaper wurde mit Hilfe von NotebookLM, Perplexity und ChatGPT erstellt.

Die Relevanz des Datenschutzes im Personalwesen

Der Datenschutz in der Personalabteilung ist ein Thema von höchster Relevanz und erfordert besondere Sorgfalt bei der Verarbeitung sensibler Mitarbeiterdaten. Er ist nicht nur eine gesetzliche Verpflichtung, sondern auch ein Ausdruck von **Integrität und Verantwortungsbewusstsein** gegenüber den Angestellten. Während die Datenschutz-Grundverordnung (DSGVO) von vielen Unternehmen nach außen hin gut umgesetzt wird, gilt sie ebenso strikt für die Verarbeitung personenbezogener Daten *innerhalb* des Unternehmens, insbesondere im HR-Bereich.

Im HR-Bereich werden hauptsächlich **Beschäftigtendaten** verarbeitet. Diese umfassen neben den Daten von Angestellten auch personenbezogene Daten, die in Bewerbungsverfahren anfallen (Bewerberdaten), sowie Daten von Arbeitnehmerüberlassungen (§ 26 Abs. 8 Nr. 1 BDSG). Zu diesen Personaldaten gehören offensichtliche Informationen wie Name, Adresse, Geburtsdatum, aber auch sensible Daten wie Gehaltsinformationen, Krankheitsgeschichten, Sozialversicherungsnummern und sogar Kommunikations- oder Zugangsdaten.

Rechtliche Grundlagen und Kernprinzipien

Der Rahmen für den Datenschutz im Personalwesen wird in Deutschland zentral durch die **Datenschutz-Grundverordnung (DSGVO)** und das **Bundesdatenschutzgesetz (BDSG)** geregelt. Die DSGVO, als Verordnung der Europäischen Union, hat Vorrang vor nationalen Gesetzen und gilt für alle EU-Mitgliedstaaten. Das BDSG ergänzt die DSGVO auf nationaler Ebene und klärt spezifische Punkte, wie etwa die Bestellung eines Datenschutzbeauftragten (§ 38 BDSG).

Datenverarbeitung im Beschäftigungskontext (§ 26 BDSG)

Die DSGVO gilt uneingeschränkt für Mitarbeiterdaten. Die maßgeblichen Vorschriften für die Verarbeitung personenbezogener Daten im Beschäftigungskontext sind in **§ 26 BDSG** festgelegt. Demnach ist die Verarbeitung rechtmäßig, wenn sie für die Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich ist.

Die Grundsätze der Datenverarbeitung (Art. 5 DSGVO)

Alle personenbezogenen Daten, die in einer Personalabteilung anfallen, unterliegen dem Schutz der DSGVO. Die folgenden Grundprinzipien müssen dabei beachtet werden:

1. **Zweckbindung:** Die Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und verarbeitet werden. Bei Beschäftigtendaten besteht der legitime Zweck beispielsweise im Mitarbeiter- oder Bewerberverhältnis. Daten werden zur Stellenbesetzung oder der Durchführung des Beschäftigungsverhältnisses verwendet.

2. **Datenminimierung:** Es dürfen nur die absolut notwendigen Daten für die Durchführung des Beschäftigungsverhältnisses verarbeitet werden. Unternehmen sollten nur so viele personenbezogene Daten wie nötig erheben, verarbeiten und speichern.

3. **Richtigkeit:** Die erhobenen Beschäftigtendaten müssen korrekt sein und bei Bedarf aktualisiert werden. Fehlerhafte Daten sind unverzüglich zu berichtigen.

4. **Speicherbegrenzung:** Personenbezogene Daten dürfen nicht unbegrenzt gespeichert werden. Nach Ablauf der gesetzlich vorgeschriebenen Aufbewahrungsfrist müssen sie gelöscht werden.

5. **Integrität und Vertraulichkeit:** Der Schutz vor unbefugter Verarbeitung oder dem unbefugten Zugriff Dritter ist wichtig. Hierfür sind technische und organisatorische Maßnahmen (TOMs) erforderlich.

6. **Rechenschaftspflicht:** Unternehmen müssen jederzeit nachweisen können, dass sie die Datenschutzprinzipien einhalten, was eine sorgfältige Dokumentation aller Verarbeitungsaktivitäten erfordert.

Verarbeitung von Mitarbeiter- und Bewerberdaten

Die Verarbeitung von Personaldaten muss stets transparent erfolgen. Mitarbeiter und Bewerber müssen umfassend über den Zweck der Datenverarbeitung, die Rechtsgrundlage und die Speicherdauer informiert werden (Informationspflicht nach DSGVO).

Zulässige und Unzulässige Daten

Grundsätzlich sind alle Informationen, die für die Begründung oder Durchführung des Beschäftigungsverhältnisses erforderlich sind (wie Bewerbungsunterlagen, Arbeitsvertragsdaten, Finanz- und Sozialversicherungsdaten), zu schützen.

Unzulässige Daten: Die DSGVO verbietet die Erhebung bestimmter Informationen in der Personalakte, die in älteren oder großen Unternehmen teilweise noch erhoben werden. Dazu gehören meist religiöse und politische Überzeugungen, sexuelle Vorlieben, Social-Media-Profile und ärztliche Unterlagen wie Atteste.

Zusätzliche Daten: Für die Verarbeitung von Daten, die über das Beschäftigungsverhältnis hinausgehen (z.B. Mitarbeiterfotos auf der Webseite, Notfallkontaktdaten), ist eine **gesonderte Rechtsgrundlage**, wie die Einwilligung der betroffenen Person, erforderlich.

Aufbewahrung und Löschung von Daten

Die Einhaltung der Speicherbegrenzung (Art. 5 DSGVO) ist eine zentrale Pflicht der Personalabteilung.

Aufbewahrungsfristen

Aufbewahrungsfristen für Personalakten nach der DSGVO existieren nicht direkt. Stattdessen richtet sich die Aufbewahrungsfrist danach, welche Dokumente in der Akte enthalten sind.

- **Reguläre Verjährungsfrist:** Endet nach drei Jahren (§ 195 BGB).
- **Steuerrechtlich relevante Unterlagen:** Müssen mindestens sechs Jahre aufgehoben werden.

Unabhängig von der Dauer muss die **Vertraulichkeit** der Akte zu jeder Zeit gewährleistet sein.

Löschungspflichten

Endet das Beschäftigungsverhältnis, müssen die personenbezogenen Daten nach der vorgeschriebenen Aufbewahrungsfrist gelöscht werden. Der Grundsatz lautet: **Nicht benötigte Daten sind unverzüglich zu löschen**.

Sonderfall Bewerberdaten (Talent-Pool): Möchte das Unternehmen Bewerberdaten über den eigentlichen Bewerbungsprozess hinaus speichern (z.B. in einem Talent-Pool), muss der Bewerber dem **ausdrücklich zustimmen**.

Datensicherheit im HR-Bereich (TOMs)

Datenschutz in der Personalabteilung beschränkt sich nicht nur auf die DSGVO, sondern umfasst auch den allgemeinen Datenschutz und die Datensicherheit. Datensicherheit ist eng mit der Unternehmens-IT verknüpft (Informationssicherheit).

Technische und Organisatorische Maßnahmen (TOMs)

Um die Integrität und Vertraulichkeit der Daten zu gewährleisten, sind spezifische Aktionen, Verfahren und Kontrollen – die TOMs – unverzichtbar. Sie schützen vor unbefugtem physischem oder digitalem Zugriff.

Beispiele für TOMs im HR-Bereich:

- **Zugangskontrollen:** Sicherstellung, dass nur befugte Mitarbeiter Zugriff auf sensible Daten erhalten.
- **Verschlüsselung:** Verschlüsselung sensibler Daten und der Daten in HR-Software.
- **HR-Software und digitale Personalakten:** Hier gelten die Vorschriften der DSGVO und des BDSG. Zur Gewährleistung der Sicherheit sind starke Authentifizierung, die Verwendung sicherer Passwörter sowie regelmäßige Updates und Sicherheitsüberprüfungen erforderlich.
- **Physische Sicherheit:** Abschließbare Personalschränke zum Schutz vor unerlaubtem physischem Zugriff.
- **Datensicherheitskonzept:** Ein individuelles, für jedes Unternehmen unerlässliches Konzept zur Informationssicherheit.

Typische Risiken und Compliance-Maßnahmen

Datenschutzverletzungen können zu erheblichen Reputationsverlusten, rechtlichen Konsequenzen und **Bußgeldern führen, die die Existenz von KMUs bedrohen können**. Viele Risiken können durch organisatorische und prozessuale Maßnahmen reduziert werden.

Sensibilisierung und Schulung

Mitarbeiter der Personalabteilung verarbeiten oftmals enorme Mengen an Beschäftigtendaten. **Mitarbeiterschulungen im Datenschutz sind essentiell** zur Sensibilisierung und zur Vermeidung von Datenschutzverletzungen durch menschliches Versagen.

Die Rolle des Datenschutzbeauftragten (DSB)

Der DSB spielt eine entscheidende Rolle für die Compliance im HR-Bereich. Ein DSB ist erforderlich, wenn in einem Unternehmen regelmäßig mehr als neun Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (§ 38 BDSG).

Zu den Aufgaben des DSB gehören: Überwachung der Einhaltung der DSGVO und des BDSG, Beratung der Geschäftsführung und Schulung der Mitarbeiter. Die Zusammenarbeit mit dem DSB erleichtert die Umsetzung aller Anforderungen an den Datenschutz.

Weitere Praxisbeispiele zur Compliance

- **Home-Office:** Erfordert besondere datenschutzrechtliche **Zusatzvereinbarungen** zum Arbeitsvertrag, da hier zusätzliche Herausforderungen für den Datenschutz bestehen.
- **Auskunftspflicht:** Arbeitnehmer haben das Recht auf Auskunft über die zu ihrer Person gespeicherten Daten (Art. 15 DSGVO). Die Personalabteilung muss einen Prozess für Auskunftsanfragen etablieren.
- **Geheimhaltungsverpflichtung:** Eine **Verschwiegenheitserklärung** ist sinnvoll, wenn mit sensiblen Daten oder innovativen Arbeitsabläufen gearbeitet wird. Sie kann Zusatz oder Bestandteil des Arbeitsvertrags sein.
- **Datenpannen:** Bei einer Datenschutzverletzung (z. B. Hackerangriff oder Verlust personenbezogener Daten) ist der Vorfall **unverzüglich**, spätestens jedoch **innerhalb von 72 Stunden**, der zuständigen **Datenschutzaufsichtsbehörde** zu melden (Art. 33 DSGVO), sofern ein Risiko für die Rechte und Freiheiten der betroffenen Personen besteht.

Eine **Benachrichtigung der betroffenen Arbeitnehmer** ist **nur erforderlich**, wenn durch die Datenpanne ein **voraussichtlich hohes Risiko** für ihre persönlichen Rechte und Freiheiten besteht (Art. 34 DSGVO). In diesem Fall muss die Information **unverzüglich** in klarer und verständlicher Sprache erfolgen.

- **Beweispflicht:** Die Personalabteilung muss jederzeit nachweisen können (Rechenschaftspflicht), dass alle Datenschutzvorschriften eingehalten werden.

Kurze Checkliste für den Datenschutz in der Personalabteilung

Zur systematischen Überprüfung und Optimierung des Datenschutzes sollten HR-Abteilungen die folgenden Punkte regelmäßig kontrollieren:

Bereich	Maßnahme	Quelle(n)
Organisation & Personal	Bestellung oder Prüfung der Notwendigkeit eines Datenschutzbeauftragten (§ 38 BDSG).	
Prozesse & Rechtmäßigkeit	Überprüfung der Datenverarbeitungsprozesse auf Einhaltung der Grundsätze (Datenminimierung, Zweckbindung).	
Datenqualität	Sicherstellung, dass alle Beschäftigtendaten richtig sind und bei Bedarf aktualisiert werden.	
Aufbewahrung	Einhaltung der Speicherbegrenzung und der gesetzlichen Aufbewahrungsfristen (Löschkonzept).	
Sicherheit (TOMs)	Einrichtung von angemessenen technischen und organisatorischen Maßnahmen (z.B. Zugangskontrollen, Verschlüsselung).	
Compliance & Schulung	Regelmäßige Schulungen der Mitarbeiter im Umgang mit personenbezogenen Daten.	
Dokumentation	Nachweisbarkeit der Einhaltung der Datenschutzprinzipien (Rechenschaftspflicht).	
Home-Office	Vorhandensein datenschutzrechtlicher Zusatzvereinbarungen zum Arbeitsvertrag.	

Quellenverzeichnis

Greschner, Marcus: Datenschutz im Personalwesen: So schützen Sie Mitarbeiterdaten.

Proliance: Datenschutz Personalabteilung.

Taborowski, Virginie: Datenschutz in der Personalabteilung: Was gilt es zu beachten?

Passende Weiterbildungen finden Sie hier:

Praxiswissen für Ihren Erfolg im Job

Erfahren Sie in unseren Weiterbildungen praktisches und aktuelles Know-how zu den Themen Arbeitsrecht, Entgeltabrechnung und Personalmanagement.
Jetzt informieren.

e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen.
Jetzt informieren und testen.

Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als Inhouse-Training.
Jetzt individuelles Angebot anfordern.

FORUM · Institut für Management GmbH · Vangerowstraße 18 · 69115 Heidelberg · Germany
Telefon: +49 6221 500-500 · Fax: +49 6221 500-555 · www.forum-institut.de