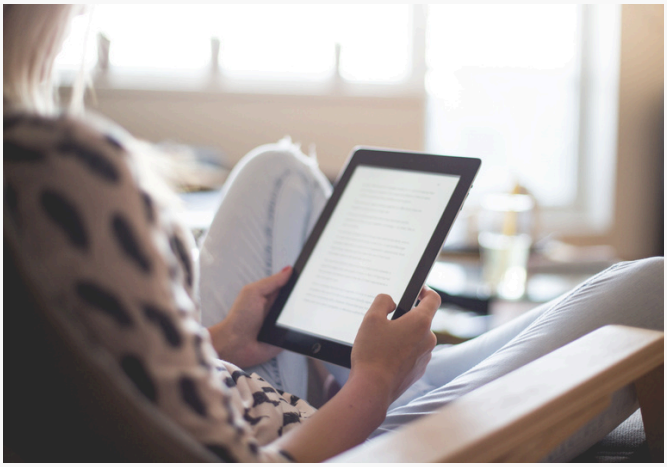
FORUM WISSEN, DAS ANKOMMT.


Leseprobe

Unsere Fachinhalte bieten Ihnen praxisnahe Lösungen, wertvolle Tipps und direkt anwendbares Wissen für Ihre täglichen Herausforderungen.

- **Praxisnah und sofort umsetzbar**: Entwickelt für Fach- und Führungskräfte, die schnelle und effektive Lösungen benötigen.
- **Fachwissen aus erster Hand**: Inhalte von erfahrenen Expertinnen und Experten aus der Berufspraxis, die genau wissen, worauf es ankommt.
- **Immer aktuell und verlässlich**: Basierend auf über 30 Jahren Erfahrung und ständigem Austausch mit der Praxis.

Blättern Sie jetzt durch die Leseprobe und überzeugen Sie sich selbst von der Qualität und dem Mehrwert unseres Angebots!

Abschließende Kontrollfragen zum Umgang der Verantwortlichen mit personenbezogenen Daten von Bewerbern[5]

- ☐ Wie kommt der Verantwortliche als potenzieller Arbeitgeber im Bewerbungsverfahren seinen Informationspflichten gem. Art. 13 DSGVO gegenüber Bewerbern nach?
- ☐ In welchen Fällen werden im Bewerbungsverfahren Rückfragen beim früheren Arbeitgeber gestellt? Auf welche Rechtsgrundlage werden diese gestützt?
- ☐ Welche Abteilungen bzw. Bereiche haben im Unternehmen Zugriff auf die Bewerbungsunterlagen und in welcher Form (elektronisch oder in Papierform)?
- ☐ Wie wird sichergestellt, dass die Bewerbungsunterlagen nach Abschluss des Bewerbungsverfahrens in den Abteilungen oder Bereichen wieder gelöscht werden?
- ☐ Wann werden die Daten der abgelehnten Bewerber gelöscht?
- ☐ Existiert im Verzeichnis der Verarbeitungstätigkeiten ein Eintrag für Bewerbungsverfahren? Falls nicht, warum nicht?

6.2.2 Durchführung des Beschäftigungsverhältnisses

Onboarding

Im Rahmen des Onboardings können Informationspflichten gegenüber dem neuen Beschäftigten erfüllt, grundlegende TOM für eine sichere Datenverarbeitung durchgeführt sowie eine erste Sensibilisierung für datenschutzrechtliche Aspekte im Unternehmen vorgenommen werden. Um den Onboarding-Prozess und zugleich eine Dokumentation der wesentlichen Punkte hinreichend zu gewährleisten, ist die Verwendung von Onboarding-Checklisten üblich. Diese können sich an den nachfolgend aufgeführten Punkten orientieren:

[5] In Anlehnung an den Fragebogen, den das BayLDA im Oktober 2018 im Rahmen einer Überprüfung an 15 größere bayerische Unternehmen und Vereine geschickt hat; vgl. https://www.lda.bayern.de/de/kontrollen.html (zuletzt aufgerufen am: 09.02.2024).

- ☐ **Information:** Neuen Mitarbeitenden müssen die nach der DS-GVO erforderlichen Informationen über die Verarbeitung seiner personenbezogenen Daten, etwa in Form eines Merkblatts, zur Verfügung gestellt werden.
- ☐ **Technische und organisatorische Maßnahmen:** Als organisatorische Maßnahme kommt insbesondere eine Verpflichtung neuer Mitarbeitender auf Vertraulichkeit beim Umgang mit personenbezogenen Daten in Betracht. Darüber hinaus sollte auf eine am „Need-to-know"-Prinzip ausgerichtete Vergabe von Zugriffsberechtigungen und auf deren Dokumentation geachtet werden. Die Ausgabe von Schlüsseln und IT-Geräten sollte entsprechend der Notwendigkeit für die jeweilige Tätigkeit der Mitarbeitenden erfolgen und ebenfalls dokumentiert werden. Auch die Einholung etwaiger Einwilligungserklärungen, z. B. in die Veröffentlichung eines Mitarbeiterfotos auf der Unternehmenswebsite, kann im Rahmen des Onboardings stattfinden.
- ☐ **Sensibilisierung:** Insbesondere wenn Mitarbeitende als Schwerpunkt ihrer Tätigkeit mit der Verarbeitung personenbezogener Daten befasst sind, sollte eine Sensibilisierung für die datenschutzrechtlichen Aspekte bereits im Rahmen des Onboardings erfolgen. Auf Arbeitsanweisungen und Richtlinien zum Datenschutz sollte hingewiesen werden, ebenso auf ein etwaiges Schulungskonzept und Kontaktmöglichkeiten mit dem Datenschutzbeauftragten.

Bei der Einholung von Einwilligungserklärungen der Beschäftigten sind nach Art. 6 Abs. 1 Satz 1 lit. a DSGVO i. V. m. § 26 Abs. 2 BDSG gesteigerte Anforderungen an die Freiwilligkeit zu beachten. Im Beschäftigungsverhältnis sind diese *„schriftlich oder elektronisch"* einzuholen – damit ist es auch möglich, datenschutzrechtliche Einwilligungen von Mitarbeitenden online im Intranet einzuholen. Dabei sollte die Rechenschaftspflicht im Blick behalten werden, d. h., die Einholung der Einwilligung sollte stets nachweisbar sein.

Softwarebasierte Verarbeitung von Beschäftigtendaten

Die Papierakte wird im Personalwesen immer mehr zum Auslaufmodell. Die softwarebasierte Verarbeitung von Mitarbeiterdaten – u. U. in einer Cloud-Lösung – ist heute nicht mehr wegzudenken. Primäres Anliegen ist dabei, eine umfassende digitale Personalar-

beit zu ermöglichen. Dabei ist allerdings zu bedenken, dass im Arbeitsrecht in zahlreichen Fällen für Dokumente die Schriftform gem. § 126 BGB vorgesehen ist, z. B. für Befristungsabreden in Arbeitsverträgen, Kündigungen oder den Nachweis der Arbeitsbedingungen nach dem NachwG.

Tipp

Aus arbeitsrechtlicher Sicht ist daher zu prüfen, welche Dokumente tatsächlich ausschließlich digital vorgehalten werden können und für welche Dokumente noch eine Aufbewahrung in Papierform erforderlich ist. Empfehlenswert ist, neben den hier behandelten datenschutz- und arbeitsrechtlichen Aufbewahrungspflichten auch solche beispielsweise nach Handels-, Gesellschafts- oder Steuerrecht separat prüfen zu lassen.

Über die reine Verwaltung von Mitarbeiterdaten hinaus ermöglichen Softwarelösungen im HR-Bereich eine Vielzahl von Verarbeitungszwecken – von Zeiterfassung, Performance-, Skill- und Learning-Management bis hin zu Zielvereinbarungen oder Vergütung. Hierbei muss stets berücksichtigt werden, dass all diese Verarbeitungsvorgänge *„zum Zwecke des Beschäftigungsverhältnisses“* erfolgen und damit, neben den Anforderungen der DSGVO an Erlaubnisgrundlage (Artt. 6, 9 DSGVO) und insbesondere Zweckänderungen (Art. 6 Abs. 4 DSGVO) unterliegen. Daneben sind die Vorgaben des § 26 BDSG (z. B. Abs. 3 i. V. m. § 22 Abs. 2 BDSG, § 26 Abs. 2 BDSG) zu beachten (► Kap. 2). Die Umsetzung dieser Anforderungen muss bereits bei Anschaffung des Systems und sodann fortlaufend erfolgen und nachgewiesen werden können.

Allgemeine datenschutzrechtliche Anforderungen

Bei der Anschaffung bzw. Einführung und der Konfiguration einer Software für die digitale Personalakte sind datenschutzrechtliche Anforderungen der DSGVO und des Beschäftigtendatenschutzes gem. BDSG von Beginn an zu berücksichtigen. Dies ergibt sich insbesondere aus den Grundsätzen von „Privacy by Design“ und „Privacy by Default“ nach Art. 25 Abs. 1 und 2 DSGVO (► Kap. 1.7.6).

Die DSGVO statuiert die Pflicht des Verantwortlichen zur Implementierung *„geeigneter technischer und organisatorischer Maßnahmen […] zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung“* (Art. 25 Abs. 1 DSGVO) daher fortlaufend ab Systemeinkauf. Zudem ist durch technische und organisatorische Maßnahmen eine Voreinstellung des Systems sicherzustellen, durch welche nur die für die jeweiligen Verarbeitungszwecke erforderlichen personenbezogenen Daten verarbeitet werden. Dies gilt für

- die Menge der erhobenen Daten,
- den Umfang ihrer Verarbeitung,
- die Speicherfrist und
- die Zugänglichkeit zu den Daten.

Zu beachten ist, dass die zu ergreifenden TOM neben dem Grundsatz der Datenminimierung auch die anderen in Art. 5 DSGVO genannten Grundsätze für die Verarbeitung personenbezogener Daten umzusetzen haben. Dies gilt auch für den Grundsatz der Rechenschaftspflicht (Abs. 2), welcher den Nachweis der Einhaltung der übrigen Verarbeitungsgrundsätze erfordert. Die datenschutzkonforme Voreinstellung des Systems und dessen datenschutzkonformer Betrieb sollten daher dokumentiert werden.

Tipp

Dementsprechend sollte die Systemeinführung in enger Abstimmung mit dem Datenschutzbeauftragten und dem IT-Sicherheitsbeauftragten erfolgen. Zudem sollte ein im Unternehmen gebildeter Betriebsrat frühzeitig miteinbezogen werden. Dies gilt auch fortlaufend für den Betrieb des Personalinformationssystems und v. a. bei der Implementierung zusätzlicher Module, die eine erweiterte und/oder umfangreichere Datenverarbeitung ermöglichen.

Dies sollte zudem vor dem Hintergrund der Prüfung der Erforderlichkeit einer Datenschutz-Folgenabschätzung berücksichtigt werden, mit der gem. Art. 35 Abs. 1 DSGVO bei hochrisikoreichen Verarbeitungsvorgängen eine *„Abschätzung der Folgen der*

vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten“ durchzuführen ist (► Kap. 5.6).

Entsprechend der – selbstverständlich auch im Beschäftigungskontext geltenden (► Kap. 2.2.5) – Transparenzanforderungen der DSGVO sind die Mitarbeitenden nach Artt. 13 und 14 DSGVO über die Datenverarbeitungsvorgänge in dem System zu informieren.

Tipp

Konkrete Empfehlungen zur Informationserteilung im Beschäftigungsverhältnis bietet der „Ratgeber Beschäftigtendatenschutz“ des LfDI BW.[6] Demnach sollten Informationen in einer für die Beschäftigten stets abrufbaren Form bereitgestellt werden, z. B. im Intranet. Eine Bestätigung der Kenntnisnahme, z. B. mittels Unterzeichnung eines Dokuments, ist hingegen nicht notwendig.

Beispiel

Die Information zu Datenverarbeitungsvorgängen innerhalb der digitalen Personalakte erfolgt mittels eines Merkblatts beim Onboarding und/oder über einen Anhang zum Arbeitsvertrag. Zudem sind diese Informationen im Intranet unter den „Informationen zum Datenschutz“ abrufbar.

Die Speicherung der personenbezogenen Daten der Mitarbeitenden muss in einer Form erfolgen, „*die die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist*“ (Art. 5 Abs. 1 lit. e DSGVO). Dies ergibt sich aus dem in Art. 5 Abs. 1 lit. e DSGVO geregelten Grundsatz der „Speicherbegrenzung“. In der Praxis sind Mitarbeiterdaten, die für statistische Zwecke verarbeitet werden sollen, zu anonymisieren. Dies gilt auch für Reportings, soweit ein Personenbezug nicht erforderlich ist.

[6] Vgl. Fußnote 1.

✎ Beispiel

Die zu Zwecken der Gehaltsabrechnung verarbeiteten Mitarbeiterdaten sollen später zur Erstellung von Gehaltsstatistiken verarbeitet werden und müssen dafür anonymisiert werden.

Die Richtigkeit von Mitarbeiterdaten ist nicht nur Voraussetzung einer funktionierenden Personalverwaltung, sondern wird mit dem Grundsatz der „Richtigkeit“ in Art. 5 Abs. 1 lit. d DSGVO als datenschutzrechtliches Grundprinzip eingefordert. Zudem müssen die Daten grds. auf dem neuesten Stand gehalten werden. Technische und organisatorische Maßnahmen müssen gewährleisten, dass unrichtige Daten unverzüglich gelöscht oder berichtigt werden.

Tipp

Wichtig ist hier, dass die systemseitigen Voraussetzungen gegeben sind, um Betroffenenrechte der Beschäftigten nach Artt. 12 ff. DSGVO (► Kap. 7) gewährleisten zu können. Es sollte bspw. möglich sein, einem Auskunftsersuchen eines Beschäftigten unkompliziert – etwa mittels Systemauszug oder Zugang durch den Beschäftigten selbst – nachkommen zu können.

Auskunftsersuchen nach Art. 15 DSGVO

Auskunftsersuchen werfen gerade im Beschäftigungskontext häufig Fragen hinsichtlich des Umfangs der zu erteilenden Auskunft auf. Schließlich sind personenbezogene Daten eines Beschäftigten nicht nur in der digitalen Personalakte gespeichert, sondern finden sich bspw. auch in der E-Mail-Korrespondenz, in Notizen des Vorgesetzten oder in Protokollen zu Meetings. Die Rechtsprechung hierzu ist uneinheitlich: Teils wurde die Auskunftspflicht des Arbeitgebers weit ausgelegt, sodass z. B. auch Vermerke zu Telefonaten und sonstigen Gesprächen mit dem Beschäftigten umfasst waren.

WISSEN, DAS ANKOMMT.

Bestelloptionen

Das Datenschutz-Paket

Sie haben Fragen zum Produkt oder benötigen Unterstützung bei der Bestellung? Unser Kundenservice ist für Sie da:

08233 / 381-123 (Mo - Do 7:30 - 17:00 Uhr, Fr 7:30 - 15:00 Uhr)

service@forum-verlag.com

Oder bestellen Sie bequem über unseren Online-Shop:

Jetzt bestellen

FORUM VERLAG HERKERT GMBH, Mandichostraße 18, 86504 Merching,
Tel.: (08233) 381 123, E-Mail: service@forum-verlag.com, Web: shop.forum-verlag.com