Der elektronische Personalakt: Was ändert die neue Datenschutzgrundverordnung?

Foto: Knyrim

Foto: Tien

© Amir Kaljikovic - Fotolia.com

Autor
Rainer Knyrim
Rechtsanwalt,
Gründer und Partner
bei Knyrim Trieb Rechtsanwälte

Autorin
Karin Tien
Rechtsanwaltsanwärterin
bei Knyrim Trieb Rechtsanwälte

Die Digitalisierung der Personalverwaltung beschäftigt HR-Abteilungen seit Jahren. Eine beinah unüberblickbare Anzahl an Softwareprogrammen lässt sich einsetzen, um HR-Prozesse digital abzubilden. Der erste Schritt besteht häufig in der Digitalisierung des Personalakts, bei der viele rechtliche Anforderungen zu beachten sind. Dieser Beitrag widmet sich den datenschutzrechtlichen Bedingungen der Umstellung auf eine elektronische Personalverwaltung und informiert über die Neuerungen, die sich durch die Datenschutzgrundverordnung ergeben.

Was ist der elektronische Personalakt?

Der „elektronische Personalakt" ist eine digitale Sammlung von Unterlagen und Dokumenten, die der Arbeitgeber über den Mitarbeiter führt. Dazu gehören üblicherweise Bewerbungsschreiben, Zeugnisse, Arbeitsverträge sowie Unterlagen zu Krankenkasse und Sozialversicherung. Der elektronische Personalakt (im Folgenden als „E-Personalakt" bezeichnet) lässt sich individuell an die Bedürfnisse einer einheitlichen Personalverwaltung anpassen. Zwingend (rechtlich) vorgesehen ist ein E-Personalakt übrigens nicht. Er kann jedoch dazu beitragen, die Personalarbeit zu erleichtern. Allerdings sind bei der Digitalisierung der Personalverwaltung sowohl arbeits- und betriebsverfassungsrechtliche Rahmenbedingungen als auch öffentlich-rechtliche Verpflichtungen, wie der Datenschutz, zu beachten.

Welche Daten dürfen Unternehmen verarbeiten?

Prinzipiell dürfen Arbeitgeber nur Unterlagen verarbeiten, die erforderlich sind, um den rechtmäßigen Zweck der Datenverarbeitung – also die Personalverwaltung – zu erfüllen. Vor Einführung des E-Personalakts sollten die HR-Abteilungen daher prüfen, welche Dokumente diesen Zweck erfüllen – und welche nicht. Dies gilt auch für den Daten-Altbestand der physischen Handakten, sofern diese in den elektronischen Personalakt übernommen werden sollen.

Eine Verarbeitung von Daten Dritter ist beispielsweise zu vermeiden. Daher sollte der Meldezettel des Mitarbeiters nicht in den Personalakt aufgenommen werden, wenn

dieser Daten des Unterkunftgebers umfasst. In diesem Fall sollte der Arbeitgeber lediglich die für die Personalverwaltung erforderlichen Informationen speichern, die der Zettel enthält.

Selbstverständlich können alle Unterlagen mit Einwilligung des Mitarbeiters in den E-Personalakt aufgenommen werden; allerdings wird im Arbeitsverhältnis die Freiwilligkeit der Einwilligung des Mitarbeiters sehr kritisch gesehen (vgl. Wolfgang Goricnik, Die Einwilligung des Arbeitnehmers als Rechtsgrundlage einer Datenverarbeitung nach der DSGVO, 2017). Im Ergebnis ist der Dienstgeber in der Pflicht, die freiwillige Erteilung der Einwilligung zu begründen. Solange andere Rechtsgrundlagen in Frage kommen, sollte man sich daher im Arbeitsverhältnis auf diese stützen.

Was darf in den E-Personalakt?

In der Praxis zeigt sich häufig, dass Arbeitgeber und HR-Verantwortliche unsicher sind, ob sie Gesundheitsdaten und behördliche Dokumente verarbeiten dürfen. Dazu zwei Beispiele:

- **Ärztliche Gutachten:** Die in ärztlichen Gutachten vorhandenen Daten zur Gesundheitssituation der Arbeitnehmer sind sensible Daten im Sinne des Datenschutzgesetzes (§ 4 Z. 2 DSG 2000), für die es einer besonderen rechtlichen Grundlage zur Verarbeitung bedarf. Andererseits ist es in Einzelfällen wohl im überwiegenden, berechtigten Interesse des Arbeitgebers, über den Gesundheitszustand der Arbeitnehmer Bescheid zu wissen, weil daran bestimmte Veränderungen des Arbeitsplatzes geknüpft sein könnten (zum Beispiel Allergien auf gewisse Chemikalien).

- **Geburtsurkunde:** Nicht alle auf der Geburtsurkunde vorhandenen Daten sind für das Arbeitsverhältnis relevant. Insbesondere ist bei volljährigen Personen nicht wichtig zu wissen, wer die Eltern sind und welchem Beruf sie nachgehen. Arbeitgeber sollten diese Unterlagen daher nicht speichern, sondern nur die daraus tatsächlich relevanten Daten, also Geburtsdatum und allenfalls Geburtsort herausschreiben und dokumentieren.

Wann ist die Datenverarbeitung rechtmäßig?

Unternehmen dürfen Mitarbeiterdaten nur verarbeiten, wenn es dafür eine Rechtsgrundlage gibt. Diese besteht, wenn gesetzliche Verpflichtungen die Verarbeitung besonders schützenswerter Daten notwendig macht. Das ist zum Beispiel dann der Fall, wenn ein Arbeitsplatz an die gesundheitlichen Einschränkungen eines Mitarbeiters angepasst werden muss. Eine Verarbeitung von Daten kann auch notwendig sein, um den Arbeitsvertrag zu erfüllen (zum Beispiel die Speicherung der Kontonummer des Arbeitnehmers, um ihm seinen Gehalt überweisen zu können) oder um berechtigte Interessen des Arbeitgebers an der Datenverarbeitung zu erfüllen (etwa die Verwendung der beruflichen Kontaktdaten des Mitarbeiters in einem Intranet-Mitarbeiterverzeichnis).

Dürfen Konzerne Daten intern weitergeben?

Das Datenschutzgesetz sieht kein allgemeines „Konzernprivileg" vor, das einen Austausch von Daten innerhalb der Konzerngruppe begünstigt. Daher liegt die Verantwortung für die rechtmäßige Verarbeitung und Übermittlung der Daten bei jenem Konzernunternehmen, das die Daten für den E-Personalakt erhoben hat. Bei dem Jobwechsel eines Mitarbeiters innerhalb eines Konzernverbundes dürfen Arbeitgeber den E-Personalakt aber auch anderen Konzernunternehmen bereitstellen. In diesem Fall ist die Weitergabe der personenbezogenen Daten zur Erfüllung vertraglicher Verpflichtungen im Sinne des Datenschutzgesetzes erforderlich und bedarf nicht der Zustimmung der Mitarbeiter (§ 8 Abs. 3 Z. 4 DSG 2000). Nichtsdestotrotz muss der Konzern den Mitarbeiter über die Daten, die das Unternehmen intern weitergibt, informieren. Ebenso speziell ist die Situation bei Beendigung eines Lehrverhältnisses, das in ein Dienstverhältnis übergeht. Da das Dienstverhältnis als Lehrling endet, dürfen Arbeitgeber die Daten nur mit Zustimmung des Mitarbeiters – sofern dieser weiterhin im Konzern beschäftigt wird – an eine andere Konzerngesellschaft weitergeben.

Wann muss das Unternehmen den Betriebsrat informieren?

Unternehmen müssen den Betriebsrat bei der Digitalisierung der Arbeitnehmerdaten einbeziehen. Bereits vor Einführung des E-Personalakts beginnt das Informationsrecht des Betriebsrats. Er muss erfahren, welche Arten von personenbezogenen Daten automationsunterstützt aufgezeichnet werden. Er wird prüfen, ob die Datenverarbeitung der Personalverwaltung oder der Kontrolle von Mitarbeitern dient. Bei der Beurteilung kommt es nicht primär darauf an, welche Daten verarbeitet werden, sondern welche Daten verarbeitet werden könnten (vgl. Remo Sacherer, Der digitale Personalakt. Ist das papierlose Personalbüro zulässig?, 2008).

Ist vor Einführung des E-Personalakts der Abschluss einer Betriebsvereinbarung notwendig?

Sofern das Personalinformationssystem das Speichern von Daten ermöglicht, die über das gesetzlich oder arbeitsvertraglich notwendige Maß hinausgehen, darf die Belegschaftsvertretung über die Einführung mitentscheiden. Unternehmen werden in diesem Fall voraussichtlich eine sogenannte

Checkliste

Einen elektronischen Personalakt einführen

- Daten-Altbestand aufbereiten (Sind diese Daten zu löschen? Dienen diese Daten tatsächlich dem Zweck der Personalverwaltung?)
- Soll-Prozess definieren und nur jene Datenarten zur Verarbeitung festlegen, die zur Mitarbeiterverwaltung zwingend erforderlich sind (Datenminimierung und Zweckbindungsgrundsatz)
- Abschluss einer Betriebsvereinbarung / Einholen der Zustimmung der Mitarbeiter
- Einführen von Löschroutinen und Festlegen der Zugriffsberechtigungen
- Abschluss einer schriftlichen Vereinbarung mit Auftragsverarbeitern
- Aufnahme der Verarbeitungstätigkeit ins Verfahrensverzeichnis
- Datensicherheitsvorkehrungen beachten und implementieren
- Mitarbeiter über die elektronische Verarbeitung ihrer Daten informieren
- Mitarbeiter im Umgang mit dem elektronischen Personalakt schulen

erzwingbare Betriebsvereinbarung abschließen müssen (gemäß § 96a Abs. 1 Z. 1 ArbVG). Dies bedeutet, dass das Unternehmen bei Nichtzustimmung des Betriebsrates die Betriebsvereinbarung vor einer Schlichtungsstelle „erzwingen" kann.

Wenn HR über das Personalinformationssystem die Leistung und/oder Persönlichkeit der Arbeitnehmer bewerten kann, gilt dies als „zustimmungspflichtige Kontrolle" (§ 96 Abs. 1 Z. 3 ArbVG). Diese macht den Abschluss einer Betriebsvereinbarung nach dem Arbeitsverfassungsgesetz unbedingt nötig, die Zustimmung des Betriebsrates kann in diesem Fall aber nicht über die Schlichtungsstelle erzwungen werden. Das heißt, bei Nichtzustimmung des Betriebsrates kann die entsprechende Software dann nicht implementiert werden (vgl. Markus Oman/Rainer Knyrim, Vom Papierakt zum ePersonalakt in der Praxis, 2014).

Sollte kein Betriebsrat vorhanden sein, ist im Falle der Implementierung von Kontrollen die Zustimmung der Arbeitnehmer einzuholen (§ 10 AVRAG).

Was ändert die Datenschutzgrundverordnung?

Bislang mussten die Unternehmen die Datenschutzbehörde regelmäßig über die Datenverarbeitung informieren. Diese Meldungen fallen ab dem 25.5.2018 weg. Nach der Datenschutzgrundverordnung sind Unternehmen mit mehr als 250 Mitarbeitern ab diesem Stichtag verpflichtet, über sämtliche Datenverarbeitungstätigkeiten selbstständig ein Verzeichnis zu führen (Art. 30 DSGVO). Unabhängig von der Anzahl der Mitarbeiter gilt die Verzeichnispflicht aber auch dann, wenn Unternehmen Gesundheitsdaten, biometrische Daten, Daten zu politischen oder weltanschaulichen Meinungen (Art. 9 Abs. 1 DSGVO) oder Daten über strafrechtliche Verurteilungen wie einen Strafregisterauszug verarbeiten (Art. 10 DSGVO), was bei einer Personalverwaltung regelmäßig der Fall ist.

Der E-Personalakt ist also als eine Verarbeitungstätigkeit in ein Verzeichnis der Verarbeitungstätigkeiten aufzunehmen. Dieses sollte sämtliche Verarbeitungen personenbezogener Daten des Unternehmens enthalten. Das Verzeichnis ist schriftlich zu führen, was

auch in einem elektronischen Format erfolgen kann.

Was sollten die Verträge zwischen Arbeitgeber und Softwarehersteller beinhalten?

Nach der Datenschutzverordnung muss der Arbeitgeber – sei es ein mittelständisches Unternehmen oder ein Konzern – mit dem Hersteller der Software für den digitalen Personalakt einen schriftlichen Vertrag abschließen. Dieser muss bestimmte inhaltliche Anforderungen erfüllen, etwa den Hersteller zur Einhaltung von Datensicherheitsmaßnahmen verpflichten oder eine Regelung zur Genehmigung von Subdienstleistern enthalten.

Wie lässt sich die Datensicherheit gewährleisten?

Der Verarbeiter von Daten ist dazu verpflichtet, in technischer und organisatorischer Hinsicht zu gewährleisten, dass eine rechtmäßige Datenverarbeitung erfolgt. Wichtige Schritte sind laut DSGVO und dem DSG 2000 die folgenden:

- Pseudonymisierung der Daten: Die Software verschlüsselt diese so, dass sie ohne Hinzuziehen zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können.
- Abschreckende, interne Disziplinarstrafen bei einem Datenschutzverstoß oder bei Nichteinhaltung von Verhaltensvorschriften (IT-Compliance)
- System zur Datenwiederherstellung im Falle des Datenverlustes (Ausfallplan)
- Installation von Antivirensoftware
- Mitarbeiterschulungen zum Thema Datenschutz
- Verwenden von Passwörtern für den Zugriffsschutz
- Verpflichtung der Mitarbeiter zur Einhaltung des Datengeheimnisses (unbedingt erforderlich!)
- Bindung der Verwendung der Daten an gültige (Arbeits-)Aufträge

Wie lassen sich die Informationspflichten erfüllen?

Laut der Datenschutzgrundverordnung haben Unternehmen im Übrigen umfassende Informationspflichten gegenüber ihren Mitarbeitern – insbesondere über nachstehende Punkte:

- Name und Kontaktdaten des Verantwortlichen für die Datenverarbeitung sowie gegebenenfalls seines Vertreters sowie des etwaigen Datenschutzbeauftragten
- Zweck und Rechtsgrundlage der Datenverarbeitung
- Verfolgte, berechtigte Interessen bei der Datenverarbeitung
- Kategorien von Empfängern der Daten (beispielsweise Behörden oder Muttergesellschaft)
- gegebenenfalls die Absicht, Daten in ein Drittland zu übermitteln, Angaben über das Datenschutzniveau im Empfängerland
- Speicherdauer der personenbezogenen Daten
- Hinweis, dass der Mitarbeiter ein Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung sowie ein Widerspruchsrecht hinsichtlich der Verarbeitung der eigenen Daten hat
- Informationen über das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde
- Möglichkeit des Widerrufs einer Einwilligungserklärung
- Mitteilung darüber, dass die Verarbeitung der Daten aus gesetzlichen Gründen erforderlich oder vertraglich vorgeschrieben ist
- Informationen über eine Weiterverwendung der Daten zu anderen Zwecken als jene, für die Daten erhoben wurden

Diese Verpflichtung kann bei Umstellung auf den E-Personalakt oftmals entfallen, wenn die Mitarbeiter über die genannten Punkte bereits ohnehin Kenntnis haben (Art. 13 Abs. 4 DSGVO), andernfalls sind diese zu informieren.

Mit Datenschutzerklärungen lässt sich sicherstellen, dass jeder Mitarbeiter über die Verarbeitung seiner Daten durch den Arbeitgeber Bescheid weiß. Eine allenfalls bereits bestehende Datenschutzerklärung sollten Unternehmen auf Vollständigkeit prüfen.

Welche Löschfristen und Speicherdauern sind gesetzlich vorgesehen?

Ein E-Personalakt erleichtert es den Arbeitgebern, die gesetzlich vorgegebenen Aufbewahrungsvorschriften einzuhalten. Bei vielen Dokumenten ist aufgrund ihrer Art ersichtlich, dass sie buchhalterisch oder abgabenrechtlich relevant sein können. Bei anderen ist dies nicht der Fall. Hier müssen die Verantwortlichen sicherstellen, dass die Daten nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Daher ist die Dauer der Aufbewahrung personenbezogener Arbeitnehmerdaten nach unterschiedlichen Gesetzesvorschriften zu beurteilen. Die Verjährungsfristen enden im Allgemeinen nach drei Jahren ab Austritt des Arbeitnehmers. Nach Ablauf dieses Zeitraums sind Mitarbeiterdaten somit zu löschen.

Fazit

Ab Mai 2018 drohen empfindliche Geldstrafen bei Verstößen gegen DSGVO-Bestimmungen (Geldbußen von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Konzernumsatzes). Daher sollten Unternehmen bei Einführung eines elektronischen Personalakts klar definieren, welche Datenarten verarbeitet werden dürfen (Grundsätze der Datenverarbeitung). Zusätzlich müssen sie die betroffenen Mitarbeiter über die Verarbeitungstätigkeit informieren und sie im Verfahrensverzeichnis (E-Personalakt) aufnehmen. Sie sollten einen Vertrag mit dem Auftragsverarbeiter (HR-Softwareunternehmen) abschließen, der die wesentlichen Eckpunkte der Zusammenarbeit definiert, sowie Zugriffberechtigungen und Löschroutinen definieren. Auch die arbeitsrechtlichen Vorschriften müssen Arbeitgeber beachten, etwa die Mitteilungspflicht an den Betriebsrat oder den Abschluss einer Betriebsvereinbarung beziehungsweise das Einholen der Zustimmung der Arbeitgeber. Nur dann können Unternehmen einen elektronischen Personalakt rechtskonform einführen.

Literaturtipps

Datenschutzrecht. Praxishandbuch für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmen, Outsourcen, Werben. Von Rainer Knyrim. Manz Verlag 2015.

Datenschutz-Grundverordnung. Das neue Datenschutzrecht in Österreich und der EU. Von Rainer Knyrim. Manz Verlag 2016.