

Typische Fälle im Beschäftigtendatenschutz

Bewerbungsverfahren

Im Rahmen von Bewerbungsverfahren stellen sich für den Bewerbenden verschiedene Fragen z.B. darüber, wie lange die schriftlichen oder elektronisch versandten Unterlagen bei dem Unternehmen aufbewahrt werden dürfen, welche Daten an sich eventuell gespeichert werden können oder wie sich Bewerber hierüber Auskunft einholen können.

1. Wen umfasst der Beschäftigtendatenschutz?

§ 26 Abs. 8 BDSG regelt in einem abschließenden Katalog, wer alles vom Beschäftigtendatenschutz erfasst wird. Hierunter fallen u.a. Arbeitnehmer/innen, Leiharbeiter/innen im Verhältnis zum Entleiher, Auszubildende und Bewerber/innen.

2. Welche Daten dürfen in Bewerberfragebögen erhoben werden?

Ein Unternehmen verwendete einen Bewerbungsbogen, mit dem eine Vielzahl von Daten abgefragt wurde. Dies umfasste u.a. Ausweis- und Reisepassnummer, Angaben zum Ehepartner (Vorname, Geburtsdatum, Beruf, Arbeitgeber), Kinder unter 18 Jahren sowie verschiedene Gesundheitsfragen (z.B. zu Kur- und Heilverfahren, schweren Krankheiten, Behinderungen), Angaben zu Rentenbezügen, derzeitiges Gehalt. Hierbei waren alle Fragen zu beantworten und Zutreffendes anzukreuzen.

Die generelle Erhebung der oben ausdrücklich genannten Daten in jedem Bewerbungsverfahren ist offensichtlich nicht für die Begründung eines Beschäftigungsverhältnisses erforderlich i.S.d. § 26 BDSG. Erhebung und Verarbeitung waren daher nicht zulässig. Die unzulässig gespeicherten Daten sind zu löschen.

3. Wie lange dürfen Bewerbungsunterlagen gespeichert werden?

Unternehmen dürfen personenbezogene Daten von Bewerber/innen für Zwecke des Beschäftigungsverhältnisses speichern, wenn dies für die Entscheidung über die Begründung des Beschäftigungsverhältnisses erforderlich ist. Bis zum Abschluss des Bewerbungsverfahrens dürfen die Daten daher gespeichert werden.

Darüber hinaus ist eine Speicherung nicht generell unzulässig. Erst wenn feststeht, dass kein Beschäftigungsverhältnis begründet wird, ist eine Löschung erforderlich. Eine Aufbewahrung für einen Zeitraum von gut zwei Monaten nach Einstellungsentscheidung ist anerkannt, § 15 Abs. 4 AGG. Innerhalb dieser Frist können abgelehnte Bewerber/Innen Ansprüche wegen einer etwaigen Benachteiligung geltend machen. Um solche Ansprüche abwehren zu können, wird die Speicherung für diesen Zeitraum als datenschutzrechtlich erforderlich i.S.d. § 26 BDSG angesehen.

Dies gilt auch für zurückgezogenen Bewerbungen. Auch hier wäre das Unternehmen ggf. in der Beweispflicht, wenn ein/e Bewerber/in eine Benachteiligung behauptet. Hierzu muss das Unternehmen zumindest das Schreiben über die Rücknahme der Bewerbung aufbewahren.

Durchführung des Beschäftigtenverhältnisses

Während des Beschäftigtenverhältnisses stellen sich vielfältige Fragen um das Thema „Überwachung am Arbeitsplatz“. Dies beinhaltet Situationen wie die Zulässigkeit von Einwilligungen im Rahmen von Beschäftigtenverhältnissen. Ist auch die private Internet- und E-Mail-Nutzung am Arbeitsplatz möglich? Kann der Arbeitgeber auf einen solchen E-Mail-Account zugreifen? Ist die Datenerhebung durch GPS/sonstige Aufzeichnung von Fahrverhalten bzw. Aufenthaltsort zulässig? Wie erfolgt die Zeiterfassung im Unternehmen und wer hat Zugriff auf die Zeiterfassungsdaten?

1. Unter welchen Voraussetzungen darf der Arbeitgeber Beschäftigtendaten erheben und verwenden?

Es gilt das sog. Prinzip des Verbots mit Erlaubnisvorbehalt. Jede Datenverarbeitung bedarf einer gesetzlichen Erlaubnis oder der Einwilligung des Betroffenen. Die DS-GVO selbst enthält für den Beschäftigtendatenschutz keine konkreten, bereichsspezifischen Regelungen. Vielmehr richtet sich der Beschäftigtendatenschutz zunächst nach den allgemeinen Regelungen der DS-GVO, die für jedes Rechtsverhältnis gelten. Der deutsche Gesetzgeber hat jedoch die Öffnungsklausel des Art. 88 Abs. 1 DS-GVO genutzt. Diese ermöglicht den Mitgliedstaaten, spezifische Vorschriften für die Verarbeitung personenbezogener Daten im Beschäftigtenkontext zu erlassen. Somit kann ein bislang höheres nationales Datenschutzniveau aufrechterhalten werden. Konkret hat der deutsche Gesetzgeber von der Öffnungsklausel durch Erlass des § 26 BDSG Gebrauch gemacht.

Diese Vorschrift findet nur im nicht-öffentlichen Bereich (Wirtschaft) Anwendung. Sie gilt also nicht für öffentliche Stellen des Bundes und der Länder (einschließlich Kommunen).

§ 26 Abs. 1 S. 1 Halbsatz 1 BDSG entspricht weitgehend der bisherigen Regelung des § 32 Abs. 1 S. 1 BDSG. Nach beiden Regelungen dürfen personenbezogene Daten von Beschäftigten für den Zweck des Beschäftigungsverhältnisses verarbeitet werden, soweit dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist.

§ 26 Abs. 1 S. 1 und Abs. 4 BDSG regelt nunmehr ausdrücklich, dass die Verarbeitung von Beschäftigtendaten auf der Grundlage von Betriebsvereinbarungen zulässig ist. Dazu gehören Tarifverträge sowie Betriebs- und Dienstvereinbarungen.

Nach § 26 Abs. 1 S. 1 Halbsatz 2 BDSG dürfen Beschäftigtendaten auch verarbeitet werden, soweit es für die Rechte und Pflichten der Interessenvertretungen der Beschäftigten erforderlich ist. Das gilt unabhängig davon, ob sich diese aus einem Gesetz, Tarifvertrag bzw. einer Betriebs- oder Dienstvereinbarung ergeben.

2. Wann sind Einwilligungen im Rahmen von Beschäftigtenverhältnisse seitens der Beschäftigten wirksam?

Hinsichtlich der Einwilligung enthält § 26 Abs. 2 BDSG eine ausdrückliche Regelung für den Beschäftigtenbereich: Beschäftigte können hiernach nur dann freiwillig in eine Datenverarbeitung einwilligen, wenn für die Beschäftigten ein rechtlicher oder wirtschaftlicher

Vorteil erreicht wird. Dasselbe gilt, wenn Arbeitgeber und Beschäftigte gleichgelagerte Interessen verfolgen.

Da der Arbeitgeber in solchen Konstellationen die Datenerhebung offenbar nicht auf eine „Erforderlichkeit für das Beschäftigtenverhältnis“ stützen kann, also die Datenerhebung für das Beschäftigtenverhältnis offenbar nicht erforderlich ist, sind an die Freiwilligkeit einer Einwilligung hohe Anforderungen zu stellen. Einwilligungen werden daher überwiegend nur in solchen Konstellationen möglich sein, die nicht das Arbeitsverhältnis als solches, sondern Zusatzleistungen des Arbeitgebers betreffen.

Zulässig sind Einwilligungen daher bei zusätzlichen Angeboten des Arbeitgebers, wie z.B. private Nutzung von Internet/E-Mail bzw. Dienst-Kfz; Aufnahme in Geburtstags-Gratulationslisten, Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung etc. Das sind folglich solche Angebote, bei denen offensichtlich ist, dass die Beschäftigten im Falle der Nichtinanspruchnahme keine negativen Auswirkungen zu befürchten haben.

Neben dem BDSG ist teilweise auch ein Rückgriff auf die DS-GVO möglich. Hierbei sind die Regelungen der DS-GVO jedoch unter Berücksichtigung der Besonderheiten des Beschäftigtenverhältnisses auszulegen. Insbesondere im Rahmen des Art. 6 DS-GVO wird die Interessenabwägung des Art. 6 Abs. 1 lit. f, Abs. 4 DS-GVO (aufgrund des besonderen Über-/Unterordnungsverhältnisses am Arbeitsplatz) grundsätzlich zu dem Ergebnis kommen müssen, dass auch für neue Verwendungszwecke noch ein innerer Zusammenhang zum Beschäftigtenverhältnis im weiteren Sinne bestehen muss. Eine Verwendung zu gänzlich anderen Zwecken (z.B. Verkauf an Dritte zu Werbezwecken) ist grundsätzlich ausgeschlossen. In solchen Konstellationen überwiegen – aufgrund des Über-/Unterordnungsverhältnisses – bei arbeitsplatzfremden Zwecken also in der Regel die Interessen, Grundrechte und Grundfreiheiten der Beschäftigten.

In diesem Zusammenhang ist auch § 24 BDSG zu beachten.

Gemäß § 26 Abs. 2 S. 3 BDSG bedarf die Einwilligung der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Gemäß § 26 Abs. 2 S. 4 BDSG hat der Arbeitgeber die Beschäftigten über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären.

3. E-Mail-/Internet am Arbeitsplatz

Siehe die ausführliche gesonderte Darstellung auf

https://www.lfd.niedersachsen.de/themen/wirtschaft/arbeitnehmer/internet_email/internet-und-e-mail-am-arbeitsplatz-146073.html

4. Darf der Arbeitgeber während der Dienstzeit den Standort seiner Arbeitnehmer mittels Tablets, Handys oder GPS im Firmenwagen ermitteln?

Einleitend: Durch die Auswertung der von GPS-Satelliten abgestrahlten und vom GPS-Empfangsgerät aufgezeichneten Signale kann festgestellt werden, zu welchem Zeitpunkt sich das Empfangsgerät, das etwa in einem von den Beschäftigten genutzten Fahrzeugen, Handys oder Tablets angebracht bzw. eingebaut ist, an welchem Ort befunden hat. Das System ermöglicht damit, den genauen Aufenthalt von Beschäftigten in ihren Firmenfahrzeugen etc. in zeitlicher und örtlicher Hinsicht permanent abzubilden und zu verfolgen. Auch wenn sich diese Angaben unmittelbar nur auf das Empfangsgerät beziehen, entsteht durch die Gerätezuordnung zu den jeweiligen Beschäftigten regelmäßig ein Personenbezug. Die Standortdaten des GPS-Empfangsgeräts enthalten daher personenbezogene Daten.

Hierzu folgende Fälle:

a) Verwendung von GPS-Ortungssystemen im Firmenfahrzeug

Ein Wartungsunternehmen stellte seinen Mitarbeitern Firmenfahrzeuge zur Erfüllung der arbeitsvertraglichen Verpflichtungen zur Verfügung. Diese waren mit einer GPS-Ortungsanlage ausgestattet. Im Bedarfsfalle griff die zuständige Stelle auf die GPS-Ortung zu, um das am nächsten befindliche Fahrzeug zum Einsatzort schicken zu können. Es erfolgte jedoch keine dauerhafte Erhebung der Positionsdaten, sondern nur bei Notwendigkeit einen dringenden Auftrag kurzfristig zu bearbeiten. Im Nachgang wurden die Positionsdaten der Fahrzeuge nicht weiter herangezogen und auch nicht gespeichert.

Für diese Standardfahrzeuge gilt: Ein „Notfall-Dispatching“ im Rahmen der Daseinsvorsorge ist mit dem Beschäftigtendatenschutz gemäß § 26 BDSG vereinbar. Die Erforderlichkeit zur Erhebung der Positionsdaten zur Durchführung des Beschäftigtenverhältnisses ergibt sich aus der Notwendigkeit, eine auftretende Störung kurzfristig zu beseitigen. Die Erhebung dient dazu, die Störung zügig durch möglichst nahe Fahrzeuge zu beseitigen.

Daneben gab es in derselben Firma Sonderfahrzeuge, welche ebenfalls mit einer GPS-Ortung ausgestattet waren, um Daten bei der späteren Abrechnung über Fahrtenprotokolle in Bezug auf An- und Abfahrten oder auch Einsatzzeiten heranzuziehen. Die Abrechnung erfolgte hier nach dem tatsächlich anfallenden Zeitaufwand. Die Positionsdaten und damit auch die genaue Einsatzzeit können dadurch zweifelsfrei belegt werden. Die durch die GPS-Ortung ermittelten Daten wurden spätestens nach der Abrechnung mit dem Auftraggeber gelöscht. Die Privatnutzung der Fahrzeuge war in der Regel nicht gestattet.

Für diese Sonderfahrzeuge gilt:

Die Erhebung der Positionsdaten und ihre zeitweilige Speicherung für Abrechnungszwecke war im konkreten, eher außergewöhnlichen Einzelfall mit § 26 BDSG noch vereinbar.

Aufgrund der besonderen Abrechnungsmodalitäten (nach Zeitaufwand), der singulären konkreten Datenspeicherung sowie der engen Zweckverwendung (nur zur Abrechnung, also nicht zu weiteren Zwecken) bestanden im Ergebnis nach Abwägung datenschutzrechtlich keine durchgreifenden Bedenken gegen die Erhebung und Speicherung der Positionsdaten. Die Erhebung ist im weiteren Sinne für die Durchführung des Beschäftigungsverhältnisses in diesem Einzelfall erforderlich.

b) Einsatz von GPS-Geräten in Taxen durch den Arbeitgeber bzw. beauftragende Taxifiliale

Ein Petent arbeitete für ein Taxiunternehmen, welches sich seinerseits einer Taxi-Zentrale angeschlossen hatte und die Fahrten durch diese Zentrale an seine Taxen vermitteln ließ. Die Zentrale nutzte hierfür ein GPS-gestütztes, automatisches Vermittlungs-System. Die Kommunikation erfolgte über ein Anzeigegerät eines anderen Unternehmens. Der Petent hatte folgende Frage: Gibt es eine Rechtfertigung dafür, dass der Disponent und andere im zentralen Raum anwesende Personen ständig die Positionen der Fahrzeuge verfolgen können?

Eine Erforderlichkeit ist zu bejahen. Die Erhebung des GPS-Signals in Taxen durch den Arbeitgeber ist, sofern er auch die Fahraufträge vermittelt, grundsätzlich zulässig. Allerdings dürfen keine unbeteiligten Personen hiervon Kenntnis nehmen können.

Grundsätzlich unzulässig ist die Erhebung des GPS-Signals in Branchen, in denen keine Disposition in Echtzeit (z.B. bei Handelsvertretern) erfolgt.

Ebenso unzulässig ist die GPS-Überwachung (mittels GPS-Handy) von Arbeitnehmern, die zu „Fuß“ unterwegs sind.

Letztlich ist auch die Erhebung von Zusatzdaten (zB Motorstatus, Drehzahlmesser, Geschwindigkeit, Dauer von Fahrtunterbrechungen) grundsätzlich unzulässig.

Hierbei handelt es sich jeweils um überschießende Informationen, die für Durchführung des Beschäftigungsverhältnisses nicht erforderlich sind.

5. Zugriff auf Personaldaten

- Zugriff auf Personaldaten auf internem Laufwerk

In einem Unternehmen wurden Informationen zum quantitativen Krankenstand vieler Mitarbeiter/innen eines Standortes unter Namensangabe auch Personen bekannt gegeben, die nicht als Vorgesetzte oder Personalsachbearbeiter/innen tätig sind. Zumindest können sämtliche Leitungspositionen des Standortes auf diese Liste zugreifen. Die Liste beinhaltet zudem Personalnummern, Namen, Standort, Stundenanzahl, Ist/Soll-Stunden, Maßnahmen und Grund der Krankheit.

Soweit der Zugriff von anderen als der jeweils vorgesetzten Leitung, deren Vertretung bzw. den Personalsachbearbeiter/innen erfolgt, wird die datenschutzrechtliche Erforderlichkeit i.S.d. § 26 BDSG zu verneinen sein.

6. Wie darf die Zeiterfassung ausgestaltet sein?

- a) In einem Fall konnten alle 100 Mitarbeiter an zwei verschiedenen Standorten „live“ sehen, ob Kollegen ein- oder ausgebucht sind. Der Arbeitgeber begründete dies mit der Notwendigkeit zügiger Kontaktaufnahme.

Grundsätzlich bestehen keine Bedenken gegen eine Darstellung von An- und Abwesenheitszeiten. Je nach Ausgestaltung und Zweck kann dies zulässig sein. Insbesondere bei größeren Einheiten kann eine An-/Abwesenheitsinformation auf Tagesbasis zulässig sein.

Erforderlich ist jedoch gerade bei großen Abteilungen bzw. Firmen, dass ausweislich Geschäftsmodell und Umfang tatsächlich in nennenswertem Maß Terminplanungen unter den einzelnen Kollegen erfolgen, die eine solche Permanentinformation sämtlicher Beschäftigten notwendig machen.

- b) In einem Unternehmen hing in einem nicht-zugangsgeschützten Büro ein Kalender mit differenzierten Angaben zu persönlich bedingten Abwesenheitszeiten (Urlaub, Krankheit mit/ohne Lohnfortzahlung).

Die Angabe der Gründe persönlich bedingter Abwesenheitszeiten müsste für die Durchführung des Beschäftigtenverhältnisses erforderlich sein. Für die Weiterleitung (Übermittlung) dieser Daten an Mitarbeiter oder externe Dritte ist die Erforderlichkeit nicht festzustellen, sofern diese keine Personalsachbearbeiter sind.

7. Darf der Arbeitgeber den Führerschein der Beschäftigten kopieren?

Ein Unternehmen fragte an, ob es berechtigt ist, die Führerscheine der Beschäftigten, die mit dem Führen von Firmenfahrzeugen beauftragt sind, zum Zweck der Kontrolle zu kopieren.

Der Arbeitgeber darf Daten der Beschäftigten erheben, verarbeiten oder nutzen, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist, § 26 BDSG. Der Arbeitgeber hat ein berechtigtes Interesse daran, sich den Führerschein einmalig bzw. regelmäßig vorzeigen zu lassen. Stammdaten wie z.B. die Führerscheinklasse kann sich der Arbeitgeber hierbei herauschreiben. Der Arbeitgeber muss jedoch darlegen, warum es ihm nicht ausreicht, sich über den – turnusmäßig - vorgezeigten Führerschein hinaus einen kurzen Vermerk zu machen („ggf. Abhaken in einer Tabelle“ etc.).

Das Kopieren des Führerscheins ist datenschutzrechtlich bedenklich. Ein Führerschein enthält, z.B. hinsichtlich eines alten Fotos, „überschießende Daten“, die der Arbeitgeber nicht benötigt. Zudem ist zu erwähnen, dass im Arbeitsverhältnis grundsätzlich nicht mit einer Einwilligung „gearbeitet werden kann“, da diese nicht freiwillig erfolgen würde i.S.d. 26 BDSG. Nicht benötigte Daten dürfen vom Arbeitgeber nicht erhoben werden. Sofern der Arbeitgeber aus besonderen Gründen im Einzelfall nachvollziehbar darlegt, dass er - über das oben genannten Herausschreiben von Daten hinaus - eine Kopie benötigt, so wären überschießende Daten zu schwärzen bzw. zur Datenminimierung mit einer entsprechenden Schablone zu kopieren.

8. Darf der Arbeitgeber eine Liste mit den Daten von schwerbehinderten Beschäftigten in einem öffentlich zugänglichen Bereich aushängen?

In einem Unternehmen wurde eine Liste für die Wahl der Schwerbehindertenvertretung ausgehängt. Auf dieser Liste standen die Namen und privaten Anschriften von etwa 90 Beschäftigten mit Schwerbehinderung. Es handelte sich um die Wahlberechtigten. Der Aushang befand sich an einem Informationsbrett im Eingangsbereich der Firma. Dieser Bereich diente den Kunden als Wartezone. Während der Öffnungszeiten konnte daher jeder Einblick in die Liste nehmen.

Nachdem die Liste abgenommen worden war, lag sie nunmehr im Personalbereich aus. Dort war sie immer noch für alle Beschäftigten einsehbar; d.h. auch für solche, die nicht wahlberechtigt waren.

Die Liste ist nach § 3 Abs. 2 SchwbVWO an geeigneter Stelle zur Einsicht auszulegen. Eine Anordnung, die Liste betriebsöffentlich auszuhängen, ist damit nicht verbunden. Mit der Schwerbehinderteneigenschaft wurden besondere Arten personenbezogener Daten bekanntgemacht. Gesundheitsbezogene Daten unterliegen als besondere Arten personenbezogener Daten einem besonderen Schutz. Der Aushang der Liste im Eingangsbereich war nach § 26 BDSG unzulässig. Auch die Einsichtsmöglichkeit durch sämtliche Beschäftigte ist unzulässig. Die Einsicht darf grundsätzlich nur durch Wahlberechtigte und Wahlbewerber erfolgen.

Auch die Ergänzung der Liste der Wahlberechtigten um deren private Anschrift war unzulässig. Die Ergänzung war weder spezialgesetzlich angeordnet noch für die Durchführung der Beschäftigtenverhältnisse gemäß § 26 BDSG erforderlich.

In diesem Fall bestand die Möglichkeit, dass durch den Aushang der Liste schwerwiegende Beeinträchtigungen für die Rechte bzw. schutzwürdigen Interessen der Betroffenen erfolgen. Es lag zugleich eine sog. Datenpanne vor. Aufgrund der drohenden schwerwiegenden Beeinträchtigungen waren neben der Aufsichtsbehörde auch die Betroffenen über diesen Verstoß zu informieren.

9. Betriebsarzt

a) Auf welche Daten darf der Betriebsarzt zugreifen?

Damit der Arbeitgeber seinen Pflichten nach dem Gesetz über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit (ASiG) erfüllen kann, muss der Betriebsarzt auf bestimmte Daten zugreifen können. Das sind jedenfalls Namen von Patienten/Beschäftigten, Art und Datum der letzten und nächsten Vorsorge sowie erstellte Arbeitsplatzbeschreibungen.

b) Wie sind die Betriebsarztakten aufzubewahren?

Die Betriebsarztakten müssen in „gehöriger Obhut“ sein. Dies kann bei einem internen Betriebsarzt auch in den Räumen des Arbeitgebers der Fall sein – dann allerdings in einer Form, die eine Kenntnisnahme des Arbeitgebers ausschließt (z.B. abgeschlossener Schrank).

c) Was geschieht mit meiner Krankenakte bei einem Betriebsarztwechsel?

Grundsätzlich ist bei der Übergabe ärztlicher Praxen an einen Rechtsnachfolger das Patientengeheimnis bezüglich der bereits vorhandenen (und im Rahmen gesetzlicher Fristen aufzubewahrenden) Patientenakten zu beachten. Der BGH hat entschieden, dass eine Praxisveräußerung einschließlich der Übertragung der Patientenakte ohne die eindeutige und unmissverständliche Einwilligung der Patienten/innen in die Weitergabe der sie betreffenden Akten wegen des Verstoßes gegen § 203 StGB i.V.m. § 134 BGB grundsätzlich unwirksam ist. Nach Auffassung des BGH verletzt eine derartige Veräußerung die ärztliche Schweigepflicht und damit das informationelle Selbstbestimmungsrecht der Patienten.

Beim Wechsel eines internen Betriebsarztes verbleiben die patientenbezogenen Unterlagen zunächst im Besitz des Arbeitgebers. Dieser darf aber, im Hinblick auf die weiterhin geltende ärztliche Schweigepflicht, keinen Einblick in die Unterlagen nehmen. Das bedeutet, dass der frühere Betriebsarzt seine Unterlagen in einem Schrank abzulegen hat, der gegen Kenntnisnahme des Arbeitgebers abgeschottet ist. Dem Arbeitgeber ist damit der Zugriff auf einzelne mitarbeiterbezogene Informationen in den Akten verwehrt. Gleichwohl behält der Arbeitgeber den Besitz an diesem abgeschlossenen Schrank als Ganzem.

Beim Wechsel eines externen Betriebsarztes sollte der frühere Betriebsarzt seine Dokumentation unmittelbar an seinen Nachfolger übergeben, zu dessen Bestellung der Arbeitgeber gesetzlich verpflichtet ist. Auf diese Weise kommt der scheidende Betriebsarzt auch seiner Verpflichtung aus § 10 Abs. 4 der Ärztlichen Berufsordnung nach, dafür Sorge zu tragen, dass seine ärztlichen Aufzeichnungen in gehörige Obhut gegeben werden.

Entsprechendes gilt, wenn elektronische Akten geführt werden. In diesem Fall müssen die Zugriffsmöglichkeiten durch entsprechende Rechtevergabe gesteuert werden.

Es besteht kein Recht des ausscheidenden Betriebsarztes daran, die Unterlagen „mitzunehmen“. Hierbei ist zu berücksichtigen, dass diese Unterlagen in der Ausübung der gesetzlichen Pflicht nach dem ASiG entstanden sind. Sie lassen sich also nicht von der Funktion loslösen, die der frühere Betriebsarzt im Rahmen seines Engagements nach § 3 ASiG hatte. Dies unterscheidet sie von den Unterlagen, die im Bereich privater ärztlicher Praxen entstanden sind. Verantwortliche Stelle i.S.d. BDSG für die Verarbeitung der in den Unterlagen enthaltenen personenbezogenen Taten ist zudem nicht der einzelne Betriebsarzt, sondern der Betrieb selbst.

10. Wie muss sich der Arbeitgeber im Falle einer Datenpanne i.S.d. Art. 33 DS-GVO verhalten?

Im vorliegenden Fall erlitt ein Unternehmen einen Angriff auf sein EDV-System. Die Backupdaten wurden gelöscht, die Originaldaten verschlüsselt und es erfolgte ein Zugriff auf die Personaldaten samt Kontoverbindungen.

Von Datenpannen spricht man dann, wenn es zu einer „Verletzung des Schutzes

personenbezogener Daten“ kommt. Eine solche Verletzung liegt vor, wenn Daten – egal ob unbeabsichtigt oder unrechtmäßig – vernichtet, verloren oder verändert werden oder wenn sie unbefugt offengelegt bzw. zugänglich gemacht werden.

Einen solchen Datenschutzverstoß müssen Sie grds. innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde melden. Entscheidend ist, dass der Verstoß unverzüglich nach Kenntnisnahme gemeldet wird. Wenn die Informationen nicht zur gleichen Zeit bereitgestellt werden können, können Sie diese ohne unangemessene weitere Verzögerung schrittweise melden.

Nach DS-GVO löst die Verletzung jeder Art von personenbezogenen Daten eine Meldepflicht aus, solange sich daraus ein Risiko für die Rechte und Freiheiten der Betroffenen ergibt. Nach DS-GVO entfällt die Meldepflicht nur dann, wenn kein oder lediglich ein geringes Risiko besteht.

Für die Meldung einer Datenpanne können Sie das Online-Meldeportal der LfD Niedersachsen verwenden.

Wenn zudem die Voraussetzungen des Art. 34 DS-GVO vorliegen (insbesondere: hohes Risiko für die Rechte und Freiheiten der Betroffenen), dann sind außerdem die Betroffenen zu informieren.

11. Welche datenschutzrechtlichen Vorgaben müssen bei einer Online-Befragung der Mitarbeiter eingehalten werden?

In einem Unternehmen sollten 400 Beschäftigte an einer Online-Befragung teilnehmen. Hierbei gilt Folgendes:

Auch bei namenslosen Befragungen gilt: Es dürfen mithilfe der möglichen Antworten (z.B. über abgefragte Standorte / Altersklassen / geschlechtsspezifische Fragen) in Verbindung mit der Größe der einzelnen angefragten Mitarbeitergruppen keine Rückschlüsse auf die Identität der einzelnen Mitarbeiter möglich sein. Erst dann kann wirklich von „anonymer Befragung“ gesprochen werden.

Für einen hinreichenden Anonymisierungsgrad müssen die Fragen und Antworten so ausgestaltet sein, dass bei jeder möglichen Antwortalternative im konkreten Fall mindestens fünf Beschäftigte in Frage kommen. Auch darf eine etwaig mögliche Kombination von Fragen und Antworten den Kreis nicht auf weniger als fünf Beschäftigte einengen.

Beziehen sich die Fragen auf besondere Arten personenbezogener Daten (z.B. Gesundheitsdaten) sollten für die möglichen Antworten mindestens 20 Beschäftigte in Frage kommen.

Auch eine Aufhebung der Anonymität durch Auswertung von IP-Adressen oder andere Zusatzdaten ist auszuschließen.

Eine nicht-anonyme Befragung müsste gemäß § 26 BDSG für die Durchführung des Beschäftigtenverhältnisses erforderlich sein, wobei sich die Erforderlichkeit hierfür regelmäßig nicht begründen lassen wird.

Zudem sollte es bei anonymen Befragungen immer die Option der Nichtteilnahme geben. Eine Verpflichtung kann sich allenfalls aus dem Arbeitsrecht ergeben.

12. Betriebliches Eingliederungsmanagement

- a) **Darf der Betriebsrat jährlich in anonymisierter Form über die Anzahl der (nicht) durchgeführten BEM-Maßnahmen unterrichtet werden?**

Hiergegen bestehen keine Bedenken, da die Daten anonymisiert sind. Voraussetzung dafür ist jedoch, dass eine Rückbeziehung auf einzelne Beschäftigte nicht möglich ist.

- b) **Welche Aufbewahrungszeit ist für BEM-Akten nach Abschluss des Eingliederungsverfahrens angemessen?**

Eine Frist für die Aufbewahrung der BEM-Unterlagen außerhalb der Personalakte ist nicht geregelt. Abhängig vom Einzelfall sind diese Daten zu löschen, wenn sie für die Durchführung des Beschäftigtenverhältnisses nicht mehr erforderlich sind. Das ist regelmäßig dann der Fall, wenn abschließend festgestellt werden kann, ob das BEM erfolgreich war oder nicht.

Eine Aufbewahrungsfrist über mehr als drei Jahre wird in der Regel nicht erforderlich sein. Spätestens nach drei Jahren sollte festgestellt worden sein können, ob das BEM erfolgreich war oder nicht.

- c) **Dürfen BEM-Daten mit der Betriebsarztakte zusammengeführt werden?**

Für die BEM-Daten besteht eine enge Zweckbindung. Diese Daten dürfen nur für das BEM verwendet werden. Eine Zusammenführung mit der Betriebsarztakte ist unzulässig.

- d) **Wer hat Zugriff auf die BEM-Unterlagen?**

Es empfiehlt sich, dass nur die mit dem BEM betrauten Personen Zugriff auf die BEM-Unterlagen nehmen können; insbesondere nicht der gesamte mit Personalangelegenheiten betraute Bereich. Sind besondere Arten personenbezogener Daten (Gesundheitsdaten/Schweigepflichtentbindungserklärung) unverschlossen in den BEM-Unterlagen enthalten, orientiert sich die Art der Aufbewahrung an den Betriebsarztakten.

Beendigung des Beschäftigtenverhältnisses

1. Gilt der Beschäftigtendatenschutz auch nach Ende des Beschäftigtenverhältnisses?

Nach § 26 Abs. 8 S. 2 BDSG erfasst der Beschäftigtendatenschutz auch Personen, deren Beschäftigungsverhältnis beendet ist.

2. Darf der Arbeitgeber im Zusammenhang mit der Beendigung des Arbeitsverhältnisses eine Liste von befristet Beschäftigten öffentlich aushängen?

Ein Personalleiter versendete eine E-Mail an insgesamt 11 Empfänger, bei denen es sich um die direkten Vorgesetzten der befristet eingesetzten Mitarbeiter handelte. Zudem leitete er diese E-Mail an drei weitere Verteilerlisten, verbunden mit der Bitte um Aushang an Informationstafeln an den verschiedenen Standorten. Inhalt der E-Mail war eine Information über eine gerichtlich nicht ersetzte Zustimmung des Betriebsrates; dessen Folge sollte die Nichtverlängerung einzelner Arbeitsverträge sein. In dieser Mail wurden die Vor- und Zunamen der betroffenen 13 Mitarbeiter sowie die einzelnen individuellen Ablaufdaten der Arbeitsverträge genannt.

Die Daten wurden unbefugt an Dritte, insbesondere Beschäftigte ohne Leitungsfunktion übermittelt. Dies verstößt gegen § 26 BDSG, da Übermittlung und Aushang für die Beendigung der Beschäftigungsverhältnisse nicht erforderlich waren.

3. Was geschieht mit Beschäftigtendaten, die noch auf dem Firmenhandy gespeichert sind?

Der Arbeitgeber hatte einem Beschäftigten ein Firmenhandy zur Verfügung gestellt, das dieser auch privat nutzen durfte. Nach einer für den Beschäftigten überraschenden Kündigung wurde ihm das Firmenhandy „abgenommen“. Trotz Protestes des Beschäftigten bekam er weder das Handy noch seine Daten „ausgehändigt“.

Das Verhalten dieses Arbeitgebers verstößt gegen § 26 BDSG. Der Arbeitgeber darf nicht kontrollieren, was mit dem Telefon „gemacht wurde“. Eine Erforderlichkeit nach § 26 BDSG lag nicht vor.

4. Auskunftsrechte ehemaliger Beschäftigter

Grundsätzlich steht ehemaligen Beschäftigten ein Auskunftsrecht über die beim Unternehmen gespeicherten personenbezogenen Daten zu.

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5
30159 Hannover
Telefon 0511 120-4500

Fax 0511 120-4599

Ihre Ansprechpartner:

E-Mail an poststelle@lfd.niedersachsen.de schreiben