W. Dalhaus /M. Dorndorf/K. Tausch/S. Tausch/K.Thönißen

Arbeitnehmerdaten richtig schützen

Grundlagen, Einzelfälle, Lösungen für die Transportbranche

VOGEL
VERLAG HEINRICH VOGEL

Arbeitnehmerdaten richtig schützen

Grundlagen, Einzelfälle, Lösungen für die Transportbranche

Inhaltsverzeichnis

In diesem Kapitel erfahren Sie, wie Sie für die relevanten Verfahren im Personalbereich den Datenschutz **umsetzen** können. Wir beginnen zunächst mit den erforderlichen vorbereitenden Schritten, welche sich später bei den einzelnen Themenpunkten (Bewerbungs- und Einstellungsverfahren, Beschäftigungsverhältnis usw.) auswirken.

Im Grundprinzip ist die Vorgehensweise im Datenschutz zu Beginn immer ähnlich:

1. Schritt: Es wird aufgenommen welche Verarbeitungen es im Unternehmen gibt, z. B. Lohn- und Gehaltsabrechnung, Zeiterfassung, etc.

Meistens ergibt sich schon automatisch daraus von welchen Personengruppen, z. B. Bewerber oder Beschäftigte, welche Kategorien von Daten (Namen, Arbeitszeiten etc.) verarbeitet werden.

2. Schritt: Hier wird u. a. geprüft, ob die jeweilige Verarbeitung sicher und vertraulich erfolgt.

Dafür ist zu prüfen, welche Personen im Unternehmen mit welchen Anwendungsprogrammen, Geräten und ggf. Dienstleistern die Daten verarbeiten.

Kommen Dienstleister zum Einsatz ist es häufig erforderlich Verträge bzw. Vereinbarungen zur Auftragsverarbeitung abzuschließen.

Da jede Verarbeitung eine Rechtsgrundlage benötigt, muss diese je Verarbeitung festgelegt werden. Je nach gewählter Rechtsgrundlage können sich neue Anforderungen ergeben, z. B. die Einholung einer Einwilligung.

3. Schritt: Nach den ersten zwei Tätigkeitsblöcken ergeben sich meistens bei der Prüfung von Verarbeitungen neue Aufgaben. Dies können einmalig erforderliche Tätigkeiten sein, wie z. B. die Einführung von neuen Sicherheitsmaßnahmen oder die Erstellung eines Dokumentes, aber auch die Anpassung von regelmäßigen Abläufen, z. B. das Aushändigen von datenschutzrelevanten Dokumenten im Rahmen des Einstellungsverfahrens.

4. Schritt: Spätestens zum Ende müssen die gewonnenen Erkenntnisse dann dokumentiert werden, sofern dies noch nicht fortlaufend während der Arbeiten erfolgt ist.

Darüber hinaus ist es ein Kreislauf, der in regelmäßigen Abständen immer wieder von vorn geprüft werden sollte, z.B. dahingehend, ob

- die Verarbeitungen noch existieren,
- neue Verarbeitungen hinzugekommen sind oder auch
- andere technische und organisatorische Maßnahmen aufgrund des Standes der Technik ergriffen werden müssen.

Absicherung von Anwendungen

Link zu Sicherheitsvorgaben des BSI für Anwendungen:

► https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_Uebersicht_node.html

Generell sollten folgende Punkte im Blick sein:

Checkliste grundlegende Sicherheitsmaßnahmen für Anwendungen

Backup:	
– Aktuelles, funktionsfähiges Backup der Daten vorhanden	
– Durchführung des Backups wird überwacht, z. B. durch Statusmeldung via E-Mail	
– Mehrere Versionen eines Backups sind vorhanden	
– Backupdatei bzw. Medium ist vom Netzwerk getrennt (wegen Verschlüsselungs-Schadsoftware)	
– Schutz vor Zerstörung, z. B. Brand, oder Diebstahl ist gegeben	
– Schutz vor Zugriff durch unbefugte Dritte, z. B. Kennwort oder Verschlüsselung, ist gegeben	
– Es ist sichergestellt, dass alle relevanten Daten gesichert werden; auch die lokal auf PCs sind	
Zugang und Zugriff:	
– Nur aktuell berechtigte Personen haben Zutritt zu den Unterlagen bzw. Geräten	
– Nur aktuell berechtigte Personen können auf die Daten (Gruppen/Benutzerrechte) oder Dokumente zugreifen (Schlüssel für Schrank etc.)	
– Direktzugriff auf die Datenbank und Export von Daten ist abgesichert	
– Schnittstellen, z. B. zur Übertragung von Daten zwischen Programmen, sind sicher	
– Es erfolgt eine angemessene Protokollierung hinsichtlich Anlage, Änderung, Löschung von Datensätzen	
– (Administrative) Standardbenutzer sind deaktiviert oder Kennwort geändert	
Wartung und Support:	
– Es erfolgt eine regelmäßige Prüfung und Installation von Updates	

Achtung: Verschlüsselungsschadsoftware

Über die Medien wird vor Online-Kriminellen mit Schadsoftware gewarnt, welche die Daten auf Computern verschlüsseln und für das Kennwort zum Entschlüsseln „Lösegeld" verlangen. Häufig wird versucht die Schadsoftware über E-Mail-Anhänge, z. B. Rechnungen oder Bewerbungen, in die Unternehmen zu bringen.
Über die Bezugnahme zu echten, aktuellen Stellenausschreibungen oder Nennung von bekannten Geschäftspartnern haben die Angreifer immer wieder Erfolg.
Hinzu kommt, dass besonders die Geschäftsleitung und Verwaltung von kleinen und mittleren Unternehmen oft lokal auf dem Computer Daten speichert. Dies sind sowohl Dateien, wie Dokumente, Kalkulationen, Bilder, etc. aber auch „Datenbanken", wie z. B. vom E-Mail-Programm, lokalen Anwendungsprogramm (Lohn- und Gehaltsabrechnung, Buchhaltung, …) etc.

nach Zweckentfall, einhalten können. Von einem unverschlüsselten Versand von sensiblen personenbezogenen Daten per E-Mail ist abzuraten. Entsprechend ist ein Versand per Post oder die persönliche Übergabe der Unterlagen an den zukünftigen Beschäftigten die praktikabelste Form.

Sofern Sie personenbezogene Daten des Beschäftigten **an einen Steuerberater oder ein externes Lohn- und Gehaltsbüro** senden, sollten Sie auch diese Datenübermittlung hinsichtlich Sicherheit und Vertraulichkeit prüfen (vgl. ► Kapitel 4.11.4). Häufig ist ein Versand entsprechender Unterlagen per E-Mail gar nicht mehr erforderlich, da die Softwareanbieter der Steuerberater und externen Lohn- und Gehaltsbüros zwischenzeitlich technische Lösungen zur Übermittlung anbieten. Diese ermöglichen z. B., entsprechende Dokumente in einem sicheren Online-Verzeichnis hochzuladen. Da sich diese Lösungen auch später im Rahmen der regelmäßigen Abrechnung nutzen lassen, sollten Sie im Bedarfsfall Ihren Steuerberater oder Dienstleister ansprechen.

Bitte beachten Sie an dieser Stelle, dass Fehlübermittlungen, sei es per Post, Fax oder E-Mail mit zu den häufigsten gemeldeten Datenschutzpannen zählen, wie die Aufsichtsbehörde Baden-Württemberg im August 2019 veröffentlichte.

Achtung: Weitergabe zwecks betrieblicher Altersvorsorge
Sofern Sie Ihren Beschäftigten eine betriebliche Altersvorsorge anbieten, sollten Sie vermeiden die Daten ihres neuen Beschäftigten an die jeweilige Versicherung, Bank oder entsprechenden Vertreter zu senden. Je nach Unternehmensgröße und Organisation bietet es sich an, dass der Anbieter entsprechende Info-Veranstaltungen durchführt und Sie diese Termine bekannt geben oder ggf. den neuen Beschäftigten mit einer Briefvorlage oder Aushang über die betriebliche Altersvorsorge informieren und darin die abgestimmten beruflichen Kontaktdaten des Anbieters hinterlegen, so dass die Initiative zur Kontaktaufnahme vom Beschäftigten ausgeht.

2.4.2 Übernahme von Unterlagen und Daten in die Personalakte

Üblicherweise übernehmen Unternehmen die kompletten Bewerbungsunterlagen in die Personalakte.

Hier stellt sich dann die Frage,

a) ob dies für den Zweck des Beschäftigungsverhältnisses wirklich erforderlich ist und
b) wenn ja, wie lange die Aufbewahrung dann erforderlich ist.

Bezüglich der Frage, **welche Daten**, jenseits des Arbeitsvertrages (z.B. Zertifikate) in einer Personalakte aufbewahrt werden müssen und dürfen, gehen auch unter Juristen die Meinungen auseinander. So stellt sich beispielsweise die Frage, ob ein Schulzeugnis, welches zumindest für den Beginn der Ausbildung als erforderlich angesehen wurde auch mehrere Jahre nach der Übernahme des Azubis noch erforderlich ist.

Sie sollten deshalb prüfen, welche Unterlagen Sie aus der Bewerbung in der Praxis überhaupt für das Arbeitsverhältnis benötigen. Für diese Dokumente sollten Sie eigene

- Geschwindigkeitsprofile,
- 4 Hz-Geschwindigkeitssignal (hiermit werden Vollbremsungen im Tachographen aufgezeichnet, es wird immer nur das letzte Ereignis aufgezeichnet).

Der Dienstleister (z.B. die Continental Automotive GmbH) wird hier als Auftragsverarbeiter nach Weisung für den Unternehmer tätig. Dazu wird regelmäßig als Annex zum Hauptvertrag über die zu beziehenden Dienstleistungen in Form eines Flottenmanagementsystems, z.B. TIS-WEB Services, zwischen Unternehmen und Dienstleister ein **Auftragsverarbeitungsvertrag** geschlossen.

Natürlich müssen die generierten Fahrzeug- und Fahrerdaten **gesetzeskonform kodiert** und sicher behandelt werden.

Der DTCO 4.0 von VDO gewährleistet dies durch ein neues kryptografisches Verschlüsselungsverfahren.

Zudem muss der Fahrer der **Weitergabe der personenbezogenen ITS- und VDO-Daten** durch entsprechendes Bestätigen **zustimmen**.

Die ITS-Schnittstelle unterscheidet dann zwischen freigegebenen und privaten Daten. Somit laufen alle Informationen in die richtigen Kanäle. Die gesicherten Datensätze zur Archivierung der Lenk- und Ruhezeiten lassen sich entsprechend von den freigegebenen Informationen trennen.

Lediglich 18 der 72 verfügbaren Datensätze sind nicht als „persönlich" klassifiziert (siehe Anhang I, Liste der über die ITS-Schnittstelle verfügbaren Daten der DVO 2016/799).

Lenk- und Ruhezeiten: Einwilligung zur Verarbeitung?

Die für die Einhaltung der Lenk- und Ruhezeiten erforderlichen Daten dürfen gemäß § 20 a Fahrpersonalverordnung (FPersVO), Art. 10 Abs. 2 VO (EG) Nr. 561/2006, Art. 7 i.V.m. 8, 9, 10, 31, 33 der VO (EU) Nr. 165/2014 verarbeitet werden. Insoweit handelt es sich um eine rechtmäßige **Verarbeitung nach Art. 6 Abs. 1 c) DSGVO**. Einer **Einwilligung** des Betroffenen zur Verarbeitung bedarf es **insoweit nicht**.

Die darüberhinausgehenden als persönlich klassifizierten Datensätze dürfen erst verwendet und verarbeitet werden, sofern der Fahrer seine Zustimmung erteilt gemäß Art. 6 Abs. 1 a) DSGVO.

3.3.3 Rechtslage zur Datenübertragung

Wie erfolgt nun die Einwilligung oder Zustimmung des Fahrers?

Unter 4.5 der Anlage 13 der DVO (EU) 2016/799 (Durchführungsverordnung „Fahrtenschreiber") heißt es insoweit:

Dem kann nicht entgegengehalten werden, dass zum Zeitpunkt des Erlasses des angegriffenen Bescheides die nunmehr maßgebliche Regelung des § 26 Abs. 2 BDSG sowie die DSGVO noch nicht existent waren. Der Klägerin hätte es frei gestanden im laufenden Verfahren von allen betroffenen Beschäftigten neue Einwilligungserklärungen einzuholen, die den aktuellen gesetzlichen Erfordernissen zur Informationspflicht entsprechen.
Ob das weitere für eine wirksame Einwilligung erforderliche Kriterium der Freiwilligkeit gegeben oder zu verneinen ist, braucht nach alledem nicht entschieden werden."

Fazit

Die Überwachung von Firmenwagen per GPS-Ortung ist nur zulässig, wenn sie für den Betriebszweck erforderlich ist oder Beschäftigte der Firma dieser wirksam zugestimmt haben.

Daneben ist zu beachten, dass der Einsatz eines flächendeckenden GPS-Ortungssystems durch das Unternehmen nicht auf die Einwilligung der Beschäftigten gestützt werden kann, da bei einer flächendeckenden Überwachung nicht von der erforderlichen Freiwilligkeit einer solchen Einwilligung der Beschäftigten ausgegangen werden kann. Die hierzu aufgestellten Grundsätze des Bundesarbeitsgerichts zur alten Rechtslage können auch mit der Anwendung der DSGVO weiterhin herangezogen werden. Die Nutzung von Ortungssystemen, mit denen das Arbeitsverhalten von Beschäftigten dauerhaft kontrolliert wird, ist datenschutzrechtlich unzulässig, da Beschäftigte keineswegs einem permanenten Kontrolldruck ausgesetzt sein dürfen.

Neue Regelung zur Datenverarbeitung im Straßenverkehrsgesetz

Zum 21. Juni 2017 ist mit § 63a Straßenverkehrsgesetz (StVG) eine neue Regelung zur Datenverarbeitung bei Kfz mit hoch- oder vollautomatisierter Fahrfunktion geschaffen worden.

Gemäß § 63 a Abs. 2 StVG dürfen Positions- und Zeitangaben, die einen Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und dem hoch- oder vollautomatisierten System protokollieren, an die für die Ahndung von Verkehrsverstößen zuständigen Behörden übermittelt werden.

Aktuell regelt § 63a Abs. 2 StVG primär einen Datenzugang zu Gunsten der Verkehrsbehörden. Insoweit heißt es:

„(die entsprechenden) Daten dürfen den (…) für die Ahndung von Verkehrsverstößen zuständigen Behörden auf deren Verlangen übermittelt werden. Die übermittelten Daten dürfen durch diese gespeichert und genutzt werden."

Schon diese grundsätzlich eingeräumte Möglichkeit birgt allerdings Probleme. Denn einen grundsätzlichen Gesetzgebungsspielraum liefert die DSGVO nach wohl zutreffender Meinung nur für die Verfolgung von **Straftaten.** Für die Ahndung von **Ordnungs-**

4.1 Telefonnutzung

4.1.1 Aufzeichnung des betrieblichen Telefonats zum Qualitätsmanagement

Sachlage

Viele Unternehmen möchten im Rahmen des Qualitätsmanagements die Telefonate eigener Mitarbeiter aufzeichnen, um diese später zum Zwecke der Servicequalität auszuwerten.

Problem

Bei der Aufzeichnung von Telefonaten mit Kunden werden nicht nur die eigenen Mitarbeiter, sondern auch die Aussagen der Kunden aufgezeichnet. Das wiederum erweitert den betroffenen Personenkreis erheblich und macht die Zulässigkeit solcher Maßnahmen komplizierter. Durch eine Aufzeichnung wird in die allgemeinen Persönlichkeitsrechte der betroffenen Personen eingegriffen, weshalb die Maßnahmen auch deshalb einer konkreten Rechtfertigung bedürfen.

Rechtslage in Bezug auf Arbeitnehmer

Grundsätzlich kann die Überwachung von Telefonaten zum Zwecke der Ausbildung, Qualitätssicherung und der Leistungskontrolle **zulässig sein, wenn** das Telefonieren des Arbeitnehmers ein wesentlicher Bestandteil seiner Arbeitsleistung ist. Die Rechtfertigung der Verarbeitung ergibt sich dann aus **Art. 6 Abs. 1, lit b) DSGVO** (in diese Richtung auch bereits vor Geltung der DSGVO: Kramer IT-ArbR B. Individualarbeitsrecht Rn. 443f.).

Zusätzlich könnte die Verarbeitung auch dadurch gerechtfertigt werden, dass der jeweilige Arbeitnehmer eine **Einwilligung erklärt**. Ungeachtet der Frage nach der Freiwilligkeit ist dies ist jedoch zum Einen nach der hier vertretenen Auffassung in der Regel nicht notwendig. Zum Anderen ist dies wegen der jederzeitigen Widerrufsmöglichkeit kaum praktikabel.

Bei der Telefonüberwachung eines Arbeitnehmers ist jedoch auch zwischen den Eingriffsarten zu differenzieren: Während

- das **heimliche** Abhören (der Arbeitnehmer hat hiervon keine Kenntnis) unzulässig ist, kann
- das **verdeckte** Abhören (sog. **„silent monitoring**“) zulässig sein.

Bei dem verdeckten Abhören weiß der Arbeitnehmer zwar, dass er abgehört wird, er kennt aber nicht den genauen Zeitpunkt. Hier ist eine intensive Verhältnismäßigkeitsprüfung durchzuführen, die den Umfang und die Intensität der jeweiligen Kontrollzeiträume begrenzt.

Schließlich gibt es noch die Variante der Aufzeichnung (sog. **„voice recording“**). Dies kann im Einzelfall zu den oben genannten Zwecken zulässig sein, wenn für den Arbeitgeber ein berechtigtes Interesse besteht und das Abhören allein nicht zweckgemäß ist. Die jeweiligen Aufzeichnungen sollten jedoch durch eine enge Zweckbindung begrenzt werden (d.h. die Festlegung konkreter Anlässe für die Aufzeichnung bzw. deren Abhören),

Das **LAG Köln** (LAG Köln, Beschluss vom 10.07.2009 – Az. 7 Ta 126/09) hat beschlossen, dass der illustrierende Charakter des Mitarbeiterfotos dann angenommen werden kann, wenn das Foto lediglich zu dekorativen Zwecken auf der Homepage verwendet wird und dem Bild keine weitere individuelle auf die Person bezogene Aussagekraft zukommt. Abgebildet war der Arbeitnehmer mit einem Telefonhörer in der Hand. Hiermit sollte die telefonische Erreichbarkeit des Unternehmen illustriert werden.

Das **BAG** (BAG, Urteil vom 11.12.2014 – Az. 8 AZR 1010/13) hat entschieden, dass auch Firmenvideos in denen beispielsweise nur Arbeitsabläufe im Betrieb dargestellt werden, reinen illustrativen Zwecken dienen.

Das **LAG Schleswig-Holstein** (LAG Schleswig-Holstein, Urteil vom 23.06.2010 – Az. 3 Sa 72/10) ging davon aus, dass die Einwilligung eines Mitarbeiters dann fortbesteht, wenn er auf dem Bild Textilien präsentiert, die von dem Arbeitgeber hergestellt werden.

Das **ArbG Frankfurt a. M.** (ArbG Frankfurt a.M., Urteil vom 20.06.2012 – Az. 7 Ca 1649/12) hat entschieden, dass ein Arbeitnehmer nicht die Entfernung des Gruppenfotos an sich verlangen kann, sondern lediglich die Unkenntlichmachung seine Abbildes auf dem Foto. Eine Unkenntlichmachung nur durch einen „schwarzen Balken" dürfte nicht genügen, vielmehr ist sein gesamtes Abbild zu verpixeln.

4.7 Social Networking und WhatsApp

4.7.1 Facebook & Co

Sachlage

Facebook, Twitter und Instagram – Social Networks sind aus dem heutigen Internet-Alltag nicht mehr wegzudenken. Die meisten Personen zeigen sich hier sehr öffentlich. An den Datenschutz denken teilweise weder die Plattformbetreiber noch die User. Gerade am Arbeitsplatz sollten solche Seiten nicht besucht werden. Und auch der Arbeitgeber ist in der Informationsbeschaffung aus Social Networks begrenzt. Für eine Überwachung des Arbeitnehmers braucht der Arbeitgeber immer eine Rechtfertigung. Denn der Datenschutz muss auch hier gewahrt werden.

Auch die gleichzeitige Nutzung von WhatsApp und Outlook auf dem beruflichen Smartphone ist heutzutage weit verbreitet. Häufig werden allerdings die damit verbundenen Haftungsrisiken übersehen oder gar ausgeblendet.

Problem Facebook & Co.

Darf der Arbeitnehmer den Rechner seines Arbeitgebers für Social Networks überhaupt verwenden? Darf der Arbeitgeber sich Informationen über den Arbeitnehmer aus Social Networks verschaffen und verwenden?

Darf der Arbeitgeber die Internetnutzung überwachen und Zugriffe auf Websites protokollieren?

Muss der Arbeitgeber technische Vorkehrung zur Unterbindung des automatischen Adressbuch-Zugriffs durch WhatsApp treffen?

Nach der Entscheidung des **EuGH** (EuGH, Urteil vom 05.06.2018 – Az. C-210/16) bedarf es für den „Status" als gemeinsamer Verantwortlicher nach Art. 26 DSGVO nur einer geringfügigen Einwirkung auf die Datenverarbeitung. Insbesondere muss nicht jeder Verantwortliche derselben Verarbeitungshandlung Zugang zu den personenbezogenen Daten haben. Dies entschied der EuGH im vorliegenden Fall im Zusammenhang mit dem Betreiben einer Facebook-Fanpage. Die Grundsätze sind aber auch auf alle anderen Bereiche anzuwenden.

4.12 Lenk- und Ruhezeiten

4.12.1 Sachlage: Aufzeichnung verpflichtend

Die Kontrolle und der Bestand der Lenk- und Ruhezeiten ist in erster Linie für die LKW-Fahrer im beruflichen Kraftverkehr gerade dem Gesetzgeber ein durchaus ernstes Anliegen. Wenn die Lenk- und Ruhezeiten nicht eingehalten werden kann auch gegenüber dem Logistikunternehmen ein Bußgeld verhängt werden. Zur Vermeidung dieser Konsequenzen, kann es für das Unternehmen von Interesse sein, diese erhobenen Daten auszuwerten und zu analysieren. In diesem Zusammenhang stellt sich dann auch die Frage, wie das Unternehmen den Datenschutzanforderungen gerecht werden kann.

Neben der Pflicht, mittels Fahrtenschreibern Daten zu erheben und die Fahrtenschreiber und Fahrerkarten regelmäßig auslesen zu lassen, müssen Unternehmer diese ausgelesenen Daten für einen bestimmten Zeitraum sicher aufbewahren. Zudem sind die Daten auf Verlangen den Behörden jeder Zeit zugänglich zu machen. Auch insoweit ist es wichtig, die Daten in einer sicheren Umgebung aufzubewahren.

4.12.2 Problem: Auswertung gesetzlich nicht geregelt

Arbeitgeber aus dem Logistikbereich sind verpflichtet, Lenk- und Ruhezeiten zu erfassen und für eine gewisse Dauer zu speichern. Daneben kann es sinnvoll sein, dass der Arbeitgeber diese Zeiten auch prüft, damit er sicherstellen kann, dass der Fahrer diese einhält. Während die Speicherung durch gesetzliche Regelungen gedeckt sein dürfte, ist die Auswertung durch den Arbeitgeber nicht gesetzlich geregelt (vgl. auch ► Kapitel 3.3).

4.12.3 Rechtslage

Die LKW-Fahrer sind grundsätzlich dazu verpflichtet, nach spätestens 4,5 Stunde eine 45 minütige Pause einzulegen. Die Einhaltung dieser Ruhezeiten wird unter anderen von dem Bundesamt für Güterverkehr und anderen zuständigen Stellen kontrolliert. Bei Verstößen kann auch der Arbeitgeber (als Weisungsgeber) in die Haftung genommen werden und es können ihn auch bei fortwährenden Verstößen verwaltungsrechtliche und sogar strafrechtliche Konsequenzen treffen. Daher besteht für ihn auch ein Interesse diese Daten

sowieso zu wahrheitsgemäßen Aussagen verpflichtet sei. Ein Bedürfnis für den Arbeitnehmer für die Überprüfung besteht also nicht (Schwarz, ZD 2018, 353). Tatsächlich wird eine weitere Überprüfung im Einzelfall dann zulässig sein, wenn objektiv Zweifel an dem Wahrheitsgehalt von Bewerbungsunteralgen bestehen; dann könnte auch der Anruf bei einem vorherigen Arbeitgeber gerechtfertigt sein.

In der Literatur wird vertreten, dass Backgroundchecks **durchaus zulässig** sein können, da der Arbeitgeber sich auch über längere Zeit an den Arbeitnehmer binde und ein gewisses Vertrauensverhältnis aufbaue (Schwarz, ZD 2018, 253, 254).

Für die tatsächliche Einstellungspraxis muss allerdings berücksichtigt werden, dass die Ansicht der Datenschutzbehörden hier eindeutig ist: danach stehen dem potentiellen Arbeitgeber mit den Bewerbungsunterlagen, möglichen Assessment-Centern und Bewerbungsgesprächen ausreichend Möglichkeiten zur Verfügung, um die Eignung des Bewerbers zu prüfen; danach bedarf es keiner Background-Checks mehr.

Der Arbeitgeber darf vorab Anfragen in verschiedenen Datenbanken bezüglich der strafrechtlichen Vorgeschichte des Arbeitnehmers stellen, sofern dies für die zu besetzende Stelle relevant ist. Dies umfasst insbesondere Einträge in sog. Sanktionslisten, da den auf diesen Listen aufgeführten Personen je nach Status nämlich keine Gehaltszahlungen oder sonstigen Gegenleistungen geleistet werden dürfen. Insoweit besteht ein berechtigtes Interesse des Arbeitgebers daran zu erfahren, ob ein Bewerber auf diesen Listen verzeichnet ist. Insbesondere für grenzüberschreitend tätige Mitarbeiter kann dies von erheblicher Relevanz sein. So ist ein Bewerber für ein Unternehmen beispielswiese „unbrauchbar", wenn die Aufgabe darin besteht, Geschäftsbeziehungen in den U.S.A. zu pflegen, der Kandidat aber auf einer sogenannten No-Fly-List steht (Lepperhoff, ZD-Aktuell 2017, 05748).

4.14.4 Einzelfälle

Der **Bundesfinanzhof** (BFH, Urteil vom 19.06.2012 – Az. VII R 43/11) hat entschieden, dass das sogenannte Sanktionslisten-Screening nach § 32 Abs. 1 S. 1 BDSG alt (somit auch nach § 26 Abs. 1 S. 1 BDSG neu) im Hinblick auf Flughafenmitarbeiter datenschutzrechtlich zulässig ist, da es für das Beschäftigungsverhältnis erforderlich ist.

Das **BAG** (BAG, Urteil vom 06.09.2012 – Az. 2 AZR 270/11) hat entschieden, dass sich eine Einschränkung des Fragerechts des Arbeitgebers im Rahmen eines Bewerbungsverfahrens auch aus dem Datenschutzrecht ergeben kann.

4.15 Arbeitsverhältnis endet – Was ist mit den Daten?

4.15.1 Sachlage: Große Datenansammlung im Zeitverlauf

Im Rahmen eines andauernden Beschäftigungsverhältnisses hat sich in der Regel eine große Anzahl an Daten über den jeweiligen Arbeitnehmer angesammelt. Insbesondere bei