LOSCHELDER

Newsletter Arbeitsrecht
Mai 2018

Inhalt

Loschelder Praxistipp:

Der datenschutzrechtliche „Beipackzettel“ zum Arbeitsvertrag

Art. 13, 14 EU-DSGVO verpflichten datenverarbeitende Stellen, gegenüber Betroffenen umfangreiche Hinweise zu erteilen, wenn sie deren personenbezogene Daten automatisiert oder in Dateisystemen verarbeitet. In sämtlichen Beschäftigungsverhältnissen kommt es zwingend zu hinweispflichtigen Datenverarbeitungsprozessen. Alle Unternehmen müssen deshalb datenschutzrechtliche Hinweisschreiben entwerfen und sämtlichen Arbeitnehmern, Auszubildenden und Praktikanten vorlegen. Dies erfolgt typsicherweise als „Beipackzettel“ zum Arbeitsvertrag.

Werden Daten automatisiert oder in Dateisystemen verarbeitet, muss die datenverarbeitende Stelle die Betroffenen **gemäß Art. 13, 14 EU-DSGVO informieren**. Dem Betroffenen müssen die Kontaktdaten des verantwortlichen Rechtsträgers, die Kontaktdaten des Datenschutzbeauftragten, der Zweck der Datenverarbeitung, die Rechtsgrundlagen, mögliche externe Empfänger sowie die bestehenden Lösch- und Aufbewahrungsfristen mitgeteilt werden. Weiter ist der Betroffene eingehend über seine Rechte zu belehren. Erfolgt die Datenerhebung beim Betroffenen selbst, ist ihm mitzuteilen, ob er zur Auskunft verpflichtet ist. Erfolgt die Datenerhebung aus anderen Quellen, sind dem Betroffenen diese Quellen mitzuteilen.

All dies gilt auch für die Datenverarbeitung in Beschäftigungsverhältnissen mit Arbeitnehmern, Auszubildenden oder Praktikanten. Selbstverständlich wäre es nicht praktikabel, Beschäftigte bei jedem Datenverarbeitungsvorgang gesondert und immer wieder aufs Neue zu informieren. Stattdessen sollte jedes Unternehmen ein Mitteilungsschreiben als einheitliches Formular erstellen, welches die vorgeschriebenen Informationen für sämtliche Datenverarbeitungsprozesse enthält, die es im Zusammenhang mit Beschäftigungsverhältnissen regelmäßig praktiziert. Dieses Mitteilungsschreiben sollte **allen Beschäftigten übergeben oder per E-Mail übermittelt** werden. Wenn zukünftig Mitarbeiter eingestellt werden, sollte das Mitteilungsschreiben **als datenschutzrechtlicher „Beipackzettel“ mit dem Arbeitsvertrag übergeben und unterzeichnet** werden.

Bislang ist weitgehend ungeklärt und in der rechtswissenschaftlichen Literatur umstritten, **wie konkret die Mitteilungen** erfolgen müssen. Es spricht viel dafür, dass sich die Mitteilung nicht in formelhaften Wendungen erschöpfen darf, sondern den Beschäftigten ein anschauliches Bild davon vermitteln muss, mit welchen Datenverarbeitungsprozessen sie im Arbeitsverhältnis konkret zu rechnen haben. Unternehmen sollten durch eine konkrete und eindeutige Information auf Nummer sicher gehen. Insbesondere muss der Beschäftigte über die Dauer sämtlicher Löschfristen informiert werden. Hierzu sollte der datenschutzrechtliche „Beipackzettel“ genau

mit den im Unternehmen geltenden Löschfristen abgestimmt werden, die im datenschutzrechtlichen Löschkonzept definiert wurden.

Wir unterstützen Sie bei der Formulierung des datenschutzrechtlichen „Beipackzettels“ und stellen Ihnen **Mustervorlagen** auf Wunsch gerne zur Verfügung.

Loschelder Praxistipp:

Datenschutz im Bewerbermanagement

Das Bewerberportal eines Unternehmens ist sein datenschutzrechtliches Aushängeschild: Durch einen flüchtigen Blick auf die Unternehmenswebseite kann sich jeder Außenstehende hier sofort ein Bild von den datenschutzrechtlichen Bemühungen eines Unternehmens verschaffen. Auf den Umgang der Unternehmen mit Bewerbungsunterlagen legen Datenschutzbehörden zudem besonderes Augenmerk. Dies überrascht nicht, geben Bewerbungsunterlagen doch einen sensiblen Einblick in das Persönlichkeitsprofil und den Werdegang einer Person. Arbeitgeber sollten der datenschutzkonformen Ausgestaltung ihres Bewerberportals deshalb Priorität einräumen.

Die Datenschutzbehörden beabsichtigen, den Umgang mit Bewerbungsunterlagen gesondert zu prüfen und haben zu diesem Zweck bereits detaillierte Prüfungsfragebögen veröffentlicht. Unternehmen müssen ihre Karriere-Webseiten und Bewerberportale anpassen, wozu wir dringend raten. Bedenken Sie, dass Datenschutzbehörden mit einem flüchtigen Blick auf die Karriere-

Webseite Ihres Unternehmens sofort ersehen können, ob sich Ihr Unternehmen mit der Implementierung von Datenschutzprozessen auseinandergesetzt hat oder ob es die neuen Anforderungen ignoriert. Jeder Datenschutzerklärung sieht man ohne weiteres an, ob sie sich noch an der alten Rechtslage oder den Anforderungen der EU-DSGVO orientiert.

Damit im Bereich des Bewerbermanagements keine datenschutzrechtlichen Verstöße festgestellt werden, sollten Arbeitgeber folgende Maßnahmen umsetzen:

1. Arbeitgeber müssen Bewerbern nach Art. 13 EU-DSGVO unbedingt einen **datenschutzrechtlichen Hinweis** geben, der über den Umgang mit Bewerberdaten, insbesondere den eingereichten Bewerbungsunterlagen, aufklärt. Dieser Hinweis sollte sichtbar auf der Karriere-Webseite eines jeden Unternehmens veröffentlicht werden und zwar so, dass er sowohl für Initiativbewerber wie auch bei Bewerbungen auf bestimmte Stellen keinesfalls übersehen werden kann.

   Auf Anfrage stellen wir Ihnen Formulare zur Verfügung, die auf den Bewerbungsprozess in Ihrem Unternehmen zugeschnitten sind.

2. Bewirbt sich ein **Bewerber auf eine bestimmte Stelle**, darf die Bewerbung nach Auffassung der Datenschutzbehörden im Grundsatz **nur** für die Entscheidung zur Besetzung genau **dieser** Stelle herangezogen werden. Im Unternehmen darf also nicht unter **Weiterleitung der Bewerbungsunterlagen** „herumgefragt“ werden, ob andere Führungskräfte Bedarf nach „solch einem Bewerber“ haben.

   Anders ist dies, wenn der Arbeitnehmer in eine solche Verwendung seiner Bewerbungsunterlagen ausdrücklich **einwilligt**. Dann ist deren Weiterleitung auch zulässig, um andere Einsatzmöglichkeiten im Unternehmen zu prüfen. Wenn Sie auf Ihrer Unternehmenswebseite ein Bewerbungsportal zur Verfügung stellen, sollten Sie für diese **Einwilligung** eine Ankreuz-Option veröffentlichen. In den Voreinstellungen darf das Kästchen noch nicht angekreuzt sein ("*opt in*" statt "*opt out*"). E-Mail-Bewerber können Sie in Stellenausschreibungen ausdrücklich dazu auffordern, im Bewerbungsanschreiben eine Einwilligung dazu abzugeben, dass die Bewerbungsunterlagen auch zur Besetzung weiterer Stellen herangezogen werden.

   Demgegenüber dürfen Sie **Initiativbewerbungen** grundsätzlich zur Besetzung sämtlicher in Betracht kommender Stellen heranziehen und ihren Inhalt sämtlichen Führungskräften bekannt geben, die in Betracht kommende Einstellungsentscheidungen treffen. Dies entspricht regelmäßig dem Willen des Initiativbewerbers.

3. Zum Umgang mit Bewerbungsunterlagen und Bewerberdaten müssen **Prozesse definiert** und in schriftlicher Form bekannt gegeben werden. Zum einen muss festgelegt werden, welche Personen in Bewerbungsunterlagen zu welchem Anlass Einsicht

nehmen dürfen. Zum anderen muss untersagt werden, dass Beteiligte zahlreiche Sicherheitskopien von Bewerbungsunterlagen erstellen, so dass diese nicht mehr überblickt werden können. Eine beliebige Weiterleitung von Bewerbungsunterlagen an alle Neugierigen und die Anfertigung beliebiger Sicherungskopien ist unter der neuen Rechtslage nicht mehr zulässig und muss ausdrücklich untersagt werden.

Zum anderen müssen **Löschfristen** für die Bewerbungsunterlagen festgelegt werden. Sobald unter keinem Gesichtspunkt mehr ein berechtigtes Interesse an der Verwahrung der Bewerbungsunterlagen besteht, muss die letzte im Unternehmen vorhandene elektronische Kopie gelöscht werden. Dies folgt aus Art. 17 EU-DSGVO.

- Bewerbungsunterlagen dürfen selbstverständlich während der Dauer des Bewerbungsverfahrens zum Zwecke seiner Durchführung gespeichert werden und müssen nicht gelöscht werden, solange keine endgültige Absage erfolgt ist.

- Nach der Absage des Bewerbers dürfen die Bewerbungsunterlagen weitere drei bis sechs Monate gespeichert werden, um sie als Beweismittel für einen möglichen Entschädigungsprozess wegen behaupteter Bewerber-Diskriminierung (vgl. § 15 Abs. 2 u. Abs. 4 AGG) vorzuhalten. Zu diesem Zeitpunkt benötigt streng genommen nur noch die Rechtsabteilung Zugriff auf die Bewerbungsunterlagen. Hierzu kann eine zentrale Datenbank mit automatisierten Löschfristen eingerichtet werden, wobei die Löschfristen bei Abschluss des Bewerbungsverfahrens „scharf“ zu schalten wären. Es spricht viel dafür, dass alle Beteiligten bei Abschluss des Bewerbungsverfahrens sämtliche sonstige elektronische Kopien der Bewerbungsunterlagen löschen und Papierausdrucke vernichten sollten.

- Bei Initiativbewerbern und Bewerbern, die einer Verwendung ihrer Bewerbungsunterlagen auch für andere Stellenbesetzungen eingewilligt haben, können die Bewerbungsunterlagen zu diesem Zweck für einen Zeitraum von ca. einem Jahr den in Betracht kommenden Entscheidern im Unternehmen zur Verfügung gestellt werden. Typischerweise werden die Bewerbungsunterlagen hierzu in einer Datenbank im Unternehmensintranet für definierte Berechtigte für den Zugriff freigegeben. Bewerbungsunterlagen, die älter als ein Jahr alt sind, entfalten für Stellenbesetzungen keine signifikante Aussagekraft mehr und dürfen zu diesem Zweck nicht mehr aufbewahrt werden. In der Bewerberdatenbank sollte deshalb eine Lösch- oder Sperrroutine implementiert werden, die nach einem Jahr automatisch ausgelöst wird.

- Datenschutzbehörden legen Wert darauf, dass sämtliche Papierausdrucke von Bewerbungsunterlagen entweder zurückgegeben oder im Aktenvernichter zerschreddert, nicht aber im normalen Müll entsorgt werden.

Die Datenschutzbehörden erwarten, dass solche Prozesse in schriftlichen Dienstanweisungen bekanntgegeben und in regelmäßigen Schulungen besprochen werden. Dass einzelne Mitarbeiter gelegentlich gegen diese Vorgaben verstoßen, lässt sich natürlich nicht vermeiden.

4. Wenn Sie **Bewerberfragebögen** verwenden, müssen die dort gestellten Fragen zulässig sein. Fragen nach Familienverhältnissen, Geburtsort, Nationalität oder Alter gelten z.B. im Grundsatz als unzulässig. Sie sollten nicht in standardisierten Bögen enthalten sein, welche womöglich auf der Unternehmenswebseite veröffentlicht werden und der Datenschutzbehörde sofort ins Auge springen.

Loschelder Praxistipp:

Anpassung von Datenverarbeitungsvorgängen – Was ist im HR-Bereich zu tun?

Unternehmen müssen zum 25.05.2018 ein EU-DSGVO-konformes Datenmanagement einführen. Mit Blick auf die Beschäftigtendaten bleibt diese Aufgabe oft an den Personalabteilungen hängen. Unsere Checkliste zeigt Ihnen, was bei der Anpassung von Personaldatenverarbeitungsprozessen zu tun ist. Die größte Herausforderung besteht in der Implementierung von Löschkonzepten.

Ein großer Teil der von Unternehmen verarbeiteten personenbezogenen Daten sind Beschäftigtendaten. Ihren Umgang mit Beschäftigtendaten sollten Unternehmen anlässlich der Geltungserlangung der EU-DSGVO unbedingt hinterfragen. Wenn der Datenschutzbeauftragte nicht aktiv wird, sollten die Personalabteilungen handeln. Orientieren Sie sich hierzu an unserer Check-Liste:

1. Sämtliche Datenverarbeitungsvorgänge im Unternehmen müssen nach Art. 30 EU-DSGVO in einem **Verzeichnis von Verarbeitungstätigkeiten** erfasst werden. Bei einer Prüfung werden die Datenschutzbehörden zuallererst diese Verzeichnisse anfordern und darin nach sensiblen Vorgängen suchen. Für den datenschutzrechtlichen Compliance-Prozess ergibt sich aus dem Verzeichnis der Verarbeitungsvorgänge die maßgebliche To-Do-Liste: Jeder der dort aufgeführten Datenverarbeitungsvorgänge muss auf seine datenschutzrechtliche Rechtfertigung hin überprüft und gegebenenfalls angepasst werden.

2. Im Ausgangspunkt stellt sich für jeden **Datenverarbeitungsvorgang** die Frage, ob er im Ganzen oder womöglich nur teilweise **gerechtfertigt** ist. Allgemein gesprochen ist zu prüfen, ob der Vorgang zum Zwecke der Durchführung des Beschäftigungsverhältnisses oder zur Verfolgung anderweitig legitimer Interessen erforderlich und verhältnismäßig ist (Art. 6 Abs. 1 lit. c u. f. EU-DSVO i.V.m. § 26 Abs. 1 Satz 1 u. 2 BDSG n.F.). Was dies im Einzelnen bedeutet, ist weitgehend unsicher. Unter dem bislang geltenden Bundesdatenschutzgesetz wurden zur datenschutzrechtlichen Rechtfertigung von Personalverarbeitungsvorgängen kaum gerichtliche Entscheidungen veröffentlicht, da das Datenschutzrecht bislang an einem Durchsetzungsdefizit litt. Dies wird sich erst nach Geltungserlangung der EU-DSGVO ändern. Bis die ersten gerichtlichen Entscheidungen veröffentlicht werden, müssen sich Arbeitgeber in vielen Punkten jedoch erst einmal auf ihr Bauchgefühl verlassen.

   Wir raten **nicht** zu **überzogener Angst vor datenschutzrechtlichen Sanktionen**. Unternehmen, die Ihre Datenverarbeitungsvorgänge systematisch hinterfragen, tun derzeit bereits mehr, als ein großer Teil ihrer Mitbewerber. Solche Unternehmen werden in den Augen der Datenschutzbehörden nicht als die „schwarzen Schafe“ erscheinen. Bevor bei bestehenden sinnvollen Datenverarbeitungsvorgängen schmerzhafte Einschränkungen vorgenommen werden, sollte besser abgewartet werden, bis sich die Rechtslage nach und nach klärt. Schon jetzt erkennen Datenschutzbehörden übrigens an, dass es grundsätzlich der unternehmerischen Freiheit des Arbeitgebers unterliegt, darüber zu entscheiden, welche Datenverarbeitungsprozesse erforderlich sind und welche nicht.

   Im Arbeitsverhältnis übliche Datenverarbeitungsvorgänge wie die Lohnbuchhaltung, die Arbeitszeiterfassung sowie das Führen einer Personalakte mit dem üblichen Inhalt (Arbeitsverträge, Bewerbungsunterlagen, Zeugnisse, Abmahnungen,

Zielvereinbarungen) dürfen selbstverständlich fortgesetzt werden.

Kritischer sollte die Gestaltung interner Mitarbeiterportale, Leistungsdokumentationen oder besonderer Überwachungsmaßnahmen hinterfragt werden. Die Ergebnisse von Mitarbeiterbefragungen und Untersuchungen sollten i.d.R. anonymisiert dokumentiert und ausgewertet werden. Bei besonders sensiblen Vorgängen sollten Unternehmen eine Datenschutz-Folgeabschätzung nach Art. 35 EU-DSGVO durchführen und schriftlich dokumentieren.

Ganz unzulässig wäre es, eine verdachtsunabhängige heimliche Dauerüberwachung von Mitarbeitern einzurichten, Geheimdossiers zu Details ihrer privaten Lebensführung auf Vorrat anzulegen oder Mitarbeiterdaten ohne Anonymisierung und Zustimmung an Datenhändler zu verkaufen. Derartige Maßnahmen kamen bei der überwiegenden Zahl der Arbeitgeber aber auch in der Vergangenheit nicht vor. Werden Unternehmen bei solchen Maßnahmen durch Datenschutzbehörden „ertappt“, muss künftig mit schmerzhaften Bußgeldsanktionen gerechnet werden.

3. Für die Einsichtnahme in bestimmte Mitarbeiterdaten, z.B. die Personalakte, die Arbeitszeiterfassung, angelegte BEM-Akten, die Lohnbuchhaltungsunterlagen oder bestimmten Angaben in elektronischen Mitarbeiterportalen müssen **Berechtigungskonzepte** definiert werden. Solche Berechtigungskonzepte haben auch in der Vergangenheit existiert, zumindest als gelebte Praxis. Bei der überwiegenden Zahl von Unternehmen dürfte kaum Anpassungsbedarf bestehen. Generell gilt: Es ist sinnvoll, eine gelebte Praxis als offizielle Richtlinie oder in Form einer Betriebsvereinbarung zu verschriftlichen, um gegenüber den Datenschutzbehörden belegen zu können, dass ein strukturierter Prozess etabliert wurde.

4. Neu ist hingegen, dass die Unternehmen für sämtliche Datentypen **Löschfristen definieren** müssen. Hierbei sind Unternehmen im Vorteil, die ihre Personalakten nicht in Papierform, sondern elektronisch führen. In der elektronischen Personalakte können **automatisierte Löschroutinen** implementiert werden, die nicht von Hand überwacht werden müssen. Spätestens, sobald sich die IT-Dienstleister auf die Vorgaben der EU-DSGVO eingestellt haben und die ersten „Update-Wellen“ überstanden sind, spricht viel dafür, von der Papierakte zur **elektronischen Personalakte** zu wechseln.

   Bei der Festlegung von Löschfristen beraten wir nach folgender Maxime: Das Wichtigste ist, dass überhaupt sachlich begründbare Löschfristen existieren. Auf keinen Fall sollten Löschfristen zu kurz bemessen werden. Werden Daten unwiederbringlich gelöscht, können sie auch in unerwarteten Notfällen nicht mehr zurückgeholt werden und das Unternehmen ist hilflos und blind. Aus unserer Sicht sollten die **Löschfristen** daher **großzügig bemessen** werden. Z.B. verjähren Ansprüche auf Betriebsrenten erst 30 Jahre nach Tod des Arbeitnehmers und können bis dahin noch durch Witwen und Waisen gerichtlich

geltend gemacht werden (§ 18a BetrAVG). Um solchen Ansprüchen entgegentreten zu können, empfehlen wir, Arbeitsvertragsunterlagen und sämtliche Dokumentationen zu Betriebsrentenbeiträgen typisiert erst 100 Jahre nach Einstellung des Arbeitnehmers zu löschen. Es wird sich mittelfristig zeigen, welche Position Datenschutzbehörden und Gerichte zu diesem großzügigen Verständnis beziehen. Für bereits unwiederbringlich gelöschte Daten ist es dann aber zu spät.

Auf Wunsch stellen wir Ihnen gerne eine Übersicht über die von uns für zulässig und zweckmäßig gehaltenen Löschfristen zur Verfügung.

Damit Löschfristen nicht leerlaufen, sollte den Mitarbeitern übrigens untersagt werden, sich weitere elektronische Kopien sensibler Beschäftigtendaten auch auf ihrem Dienstrechner anzufertigen. Dieses Verbot sollte in schriftlichen Dienstanweisungen veröffentlicht werden.

5. Wenn Unternehmen Personaldatenverarbeitungen, insbesondere die Lohnbuchhaltung, durch einen Drittdienstleister vornehmen lassen, handelt es sich um eine **Auftragsverarbeitung** (früher: „AuftragsDATENverarbeitung“). Hierbei muss das Unternehmen mit dem Drittdienstleister einen schriftlichen Vertrag zur Auftragsverarbeitung schließen, der die Vorgaben nach Art. 28 Abs. 3 EU-DSGVO erfüllt. Altverträge mit Auftragsdatenverarbeitern nach § 11 BDSG a.F. müssen an die neue Rechtslage angepasst werden.

   Erfolgt die Personaldatenverarbeitung **konzernübergreifend** in einer Personalabteilung des Mutterunternehmens auch für verschiedene Tochterunternehmen, treten Mutter- und Tochterunternehmen als **gemeinsame Verantwortliche** nach Art. 26 EU-DSGVO auf. Hierbei müssen die wechselseitigen Rechte und Pflichten in einer besonderen, schriftlichen Vereinbarung festgelegt werden.

   Kommt es zu einer Überprüfung durch die Datenschutzbehörde, sollte Ihr Unternehmen die vorgeschriebenen schriftlichen Verträge vorlegen können. Bei der Vertragsgestaltung können Sie auf unsere lösungsorientierte Unterstützung vertrauen. Insbesondere, wenn Sie Daten ins außereuropäische Ausland übermitteln, sollten Sie sich **rechtlich beraten** lassen.

6. Beschäftigte genießen hinsichtlich erhobener personenbezogener Daten nach Art. 15 ff. EU-DSGVO eine Reihe von Rechten, nämlich auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragung und Widerspruch. Für den Fall, dass derartige Rechte geltend gemacht werden, müssen **Zuständigkeiten und Prozesse definiert** werden. Zuständigkeiten und Prozesse müssen ebenfalls feststehen, wenn personenbezogene Daten derart verletzt werden, dass gemäß Art. 33 EU-DSGVO eine Meldung bei der Datenschutzbehörde zu erfolgen hat.

Loschelder Praxistipp:

Neue Anforderungen an die datenschutzrechtliche Einwilligung

Wir raten allen Arbeitgebern, bei ihren Mitarbeitern vorsorgliche Einwilligungen für die bestehenden Datenverarbeitungsvorgänge einzuholen. Bei der Gestaltung der Einwilligungserklärungen ist Vorsicht geboten. Diese dürfen künftig nicht mehr als Vertragsbestandteil in den Arbeitsvertrag integriert werden. Stattdessen müssen für die Einwilligungserklärungen gesonderte Formulare entwickelt werden. Prüfen Sie daher Ihre Vertragsunterlagen!

Ab Inkrafttreten der EU-DSGVO wird über längere Zeit eine große Rechtsunsicherheit bei der Frage bestehen, welche Datenverarbeitungsvorgänge zulässig sind und welche nicht. Die meisten Datenschutzbehörden werden zunächst eine eher restriktive Linie vertreten, die durch Gerichte erst nach und nach korrigiert und gelockert wird. In der Zwischenzeit kann es zu kontroversen Verhandlungen zwischen Unternehmen und Datenschutzbehörden kommen. Erfahrungsgemäß sind viele Datenschützer Idealisten, die dazu neigen, über ihr Ziel hinauszuschießen.

In den Verhandlungen mit den Datenschutzbehörden kann ein Unternehmen seine Verhandlungsposition deutlich verbessern, wenn es seine Mitarbeiter in sämtliche bestehenden Datenverarbeitungsprozesse **vorsorglich einwilligen** lässt. Datenverarbeitungsprozesse, in die ein Mitarbeiter eingewilligt hat, sind nach Art. 6 Abs. 1 lit. a EU-DSGVO grundsätzlich gerechtfertigt. Will die Datenschutzbehörde Legitimationswirkung einer Einwilligung in Frage stellen, muss sie deutlich gewichtigere Einwände vorbringen.

Will ein Arbeitgeber die **Privatnutzung des Dienstrechners**, insbesondere des E-Mail-Postfachs zulassen, sollte er im Gegenzug unbedingt eine spezielle **datenschutzrechtliche Einwilligung** einholen, welche **Zugriffe des Arbeitgebers** auf die auf dem Dienstrechner gespeicherten Daten **legitimiert**. Andernfalls wären solche Zugriffe mit hohen rechtlichen Risiken bis hin zu Strafbarkeit verbunden.

Bei der Gestaltung von Einwilligungserklärungen muss der Arbeitgeber unbedingt die neu anzuwendenden **Formvorschriften** beachten:

- Die datenschutzrechtliche Einwilligungserklärung darf **nicht Bestandteil des Arbeitsvertrages** sein. Zumindest theoretisch muss der Arbeitnehmer die Möglichkeit haben, den Arbeitsvertrag zu unterzeichnen, die Abgabe der datenschutzrechtlichen Einwilligung aber zu verweigern. Dies folgt aus Art. 7 Abs. 2 u. 4 i.V.m. Erwägungsgrund 43 EU-DSGVO und § 26 Abs. 2 Satz 2 u. 3 BDSG n.F.

- Die datenschutzrechtliche Einwilligungserklärung unterliegt künftig noch **strengeren Transparenzanforderungen**. Der Arbeitgeber muss nachvollziehbar und anschaulich erläutern, auf welche Datenverarbeitungsprozesse sich die Einwilligung bezieht und zu welchen Zwecken diese erfolgen. Auch die durch die Einwilligung begünstigten Rechtsträger müssen benannt werden. Dies folgt aus Art. 7 Abs. 2 u. 4 i.V.m. Erwägungsgrund 42 EU-DSGVO und § 26 Abs. 2 BDSG n.F.

- Bei einer **vorsorglichen Einwilligung** muss unbedingt der vorsorgliche Charakter im Einwilligungsschreiben deutlich gemacht werden. Es muss nachvollziehbar klargestellt werden, dass die Datenverarbeitung auch bei Verweigerung der Einwilligung erfolgen wird und die Einwilligung nur eine zusätzliche Vorsichtsmaßnahme ist. Andernfalls werten Datenschutzbehörden die Einwilligung als irreführend.

Prüfen Sie, ob die von Ihnen bislang verwendeten Formulare diesen Anforderungen genügen. Wir stellen Ihnen gerne Formulare zur Verfügung, die auf die künftige Rechtslage und die Besonderheiten Ihres Unternehmens zugeschnitten sind.

Loschelder Praxistipp:

Schließen Sie Betriebsvereinbarungen zum Beschäftigtendatenschutz!

Nach Art. 88 EU-DSGVO und § 26 Abs. 4 BDSG n.F. können Betriebsvereinbarungen als besondere datenschutzrechtliche Ermächtigungsgrundlagen fungieren, die dazu geeignet sind, Personaldatenverarbeitungsprozesse zu legitimieren. Außerdem dokumentieren schon Verhandlungen um den Abschluss von Betriebsvereinbarungen die datenschutzrechtlichen Bemühungen eines Unternehmens eindrücklich. Wir empfehlen kurzfristig, dem Betriebsrat den Abschluss einer allgemeinen Betriebsvereinbarung zum Beschäftigtendatenschutz anzubieten.

Das Datenschutzrecht ist ein weiches Rechtsgebiet. Zwar gibt es eine Reihe von Formalvorgaben und offensichtlicher No-Gos. Oft handelt es sich aber um eine schwer zu beantwortende Wertungsfrage, ob, wieweit und auf welche Weise Unternehmen ihre Prozesse nach den Grundsätzen der Datenvermeidung und Datensparsamkeit optimieren müssen und sollten. Ausgehend von diesem Problem sehen sich **Datenschutzbehörden in einer Doppelrolle**, nämlich einerseits **als Sanktionierungs-Stelle und andererseits als Beratungs-Stelle**.

- Werden Unternehmen bei offener Ignoranz gegenüber datenschutzrechtlichen Problemstellungen „ertappt“, verhängen Datenschutzbehörden künftig in ihrer Rolle als Sanktionierungs-Stelle empfindliche **Bußgelder**.

- Ziel aller Unternehmen sollte daher sein, ersthafte Bemühungen um die datenschutzrechtliche Optimierung ihrer Prozesse zu demonstrieren; gelingt dies glaubhaft, werden Datenschutzbehörden regelmäßig von der Rolle als Sanktionierungs-Stelle in ihre Rolle als Beratungs-Stelle wechseln und **kooperativ** auf das Unternehmen zugehen.

Indem das Unternehmen ernsthafte **Verhandlungen mit seinen Betriebsräten** aufnimmt, um die Datenverarbeitungsprozesse in Beschäftigungsverhältnissen in Betriebsvereinbarungen zu regeln, kann es den Datenschutzbehörden seine **Bemühungen** um eine ausgewogene Lösung **glaubhaft demonstrieren**. Wenn der Verhandlungsprozess mit dem Betriebsrat bei bestimmten Problemfeldern ins Stocken gerät und es vorerst nicht zu einem Abschluss kommt, lässt sich gegenüber Datenschutzbehörden (immerhin) präzise und konstruktiv darstellen, wo Beratungs- und Schlichtungsbedarf besteht und in welchen Konflikten etwaige Umsetzungsverzögerungen (unverschuldet) ihre Ursache haben.

Gelingt sogar der Abschluss einer **Betriebsvereinbarung**, kann diese gemäß Art. 88 EU-DSGVO als **Ermächtigungsgrundlage** für die darin beschriebenen Datenverarbeitungsprozesse fungieren. In der Betriebsvereinbarung beschriebene Datenverarbeitungsvorgänge werden i.d.R. als datenschutzrechtlich legitimiert anzusehen sein und müssen von den Datenschutzbehörden akzeptiert werden.

Bei technischen Überwachungsmaßnahmen müssen nach § 87 Abs. 1 Nr. 6 BetrVG ohnehin Betriebsvereinbarungen geschlossen werden. Hier sollte in den Betriebsvereinbarungen klargestellt werden, dass sie zugleich datenschutzrechtliche Ermächtigungsgrundlage sind. Als Ermächtigungsgrundlage bieten sich Betriebsvereinbarungen darüber hinaus z.B. an für

- Veröffentlichung privater Angaben in Mitarbeiterlisten zu Zwecken des sozialen Austauschs,
- Taschenkontrollen,
- Einholung von Schufa-Auskünften über Mitarbeiter,
- Durchsuchungen von Schreibtischschubladen und Spints und
- den Einsatz von Scheinkunden zur Qualitätskontrolle.

Wir empfehlen, der Betriebsratsseite kurzfristig den Abschluss einer **allgemeinen** (Rahmen-) **Betriebsvereinbarung zum Beschäftigtendatenschutz** anzubieten, die „als erster Schritt“ grundsätzliche, aber dafür umfassende Regelungen enthält. Anschließend können besondere datenschutzrechtliche Problemstellungen in weiteren Verhandlungen nach und nach aufbereitet werden.

Einen **auf Ihr Haus angepassten Text** für eine allgemeine Betriebsvereinbarung zum Beschäftigtendatenschutz, die Handlungswillen demonstriert, ohne die Handlungsfähigkeit des Unternehmens zu bedrohen, können wir Ihnen zur Verfügung stellen.

Unser Team Arbeitsrecht

Dr. Detlef Grimm
+49 (0) 221 650 65-129
detlef.grimm@loschelder.de

Dr. Martin Brock
+49 (0) 221 650 65-233
martin.brock@loschelder.de

Dr. Sebastian Pelzer
+49 (0) 221 650 65-263
sebastian.pelzer@loschelder.de

Arne Gehrke, LLM.
+49 (0) 221 650 65-263
arne.gehrke@loschelder.de

Dr. Stefan Freh
+49 (0) 221 650 65-129
stefan.freh@loschelder.de

Dr. Jonas Kühne
+49 (0) 221 650 65-129
jonas.kuehne@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de