

Arbeitnehmerdatenschutz

Mit der europäischen Datenschutz-Grundverordnung wird der Datenschutz in der Europäischen Union auf eine neue Grundlage gestellt. Die EU verfügt auch in Zukunft über ein hohes Datenschutzniveau. Die Verordnung gibt dem nationalen Gesetzgeber die Möglichkeit, bestimmte Sachverhalte landesspezifisch regeln zu können. Deutschland hat im Rahmen der Anpassung des Bundesdatenschutzgesetzes (BDSG) an die Vorgaben der Datenschutz-Grundverordnung insbesondere in § 26 BDSG Regelungen für den Beschäftigtendatenschutz getroffen. In der weiteren Entwicklung müssen spezifische Einschränkungen des Datenschutzrechts auf ihre Sinnhaftigkeit überprüft werden. Digitalisierung und in deren Folge die Verarbeitung großer Datenmengen müssen durch die gesetzlichen Regelungen angemessen flankiert werden. Gesetzliche Vorgaben dürfen der Verarbeitung und Weiterverwendung solcher Daten nicht entgegenstehen. Sie müssen Beschäftigten und Arbeitgebern helfen, diese Daten zu nutzen und in Chancen für Betriebe und Beschäftigte umzuwandeln.

Kollektivvereinbarungen flexibel gestalten

Auch zukünftig können Daten weiterhin auf der Grundlage von Kollektivvereinbarungen wie Betriebsvereinbarungen und Tarifverträge verarbeitet werden. Diese Instrumente haben sich in der Praxis bewährt, denn vor allem Betriebsvereinbarungen werden vielfach genutzt, um zwischen Arbeitgebern und Arbeitnehmervertretern konkrete datenschutzrechtliche Regelungen zu treffen. Sie dürfen nicht übermäßig durch neue Vorgaben belastet werden.

Einwilligungsmöglichkeit für Arbeitnehmer weiter geben

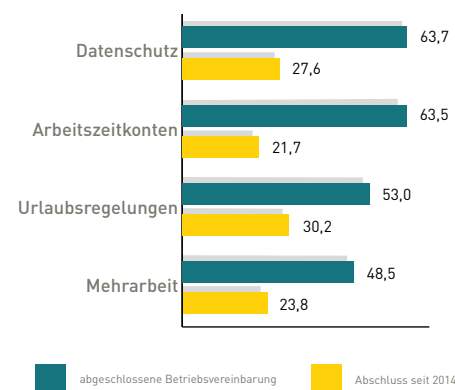
In Betrieben und Unternehmen, in denen kein Betriebsrat existiert, oder für Arbeitnehmer, die nicht in den Geltungsbereich des Betriebsverfassungsgesetzes fallen, ist die Möglichkeit unverzichtbar, in die Datenerhebung, -nutzung und -verarbeitung einwilligen zu können. Eine solche Einwilligung ist Ausdruck der Privatautonomie der Arbeitnehmer, weshalb es wichtig ist, dass die Datenschutz-Grundverordnung und das BDSG weiterhin die Erteilung einer Einwilligung im Beschäftigungsverhältnis zulässt. Bedenklich sind gleichwohl neue, unklare Vorgaben, die Arbeitgeber und Beschäftigte überfordern. Das gilt insbesondere für die Frage, wann eine Einwilligung freiwillig erfolgt.

Praxisnaher Datenschutz ist wichtig

Die Betriebe benötigen einen praxisnahen Datenschutz. Das setzt die Möglichkeit einer Modifizierung und Anpassung an die jeweiligen Gegebenheiten von Betrieb und Unternehmen voraus. Betriebsvereinbarungen zum Datenschutz im Betrieb sind deshalb von besonderer Bedeutung. Sie dürfen nicht übermäßig durch neue Vorgaben belastet werden.

Bewährtes Instrument: Betriebsvereinbarungen zum Datenschutz

Themen von Betriebsvereinbarungen, Angaben in Prozent



Quelle: WSI, 2016

Konzerndatenschutz ins Auge gefasst

Für Konzernunternehmen ist der Austausch von Daten unverzichtbar. Innerhalb von Konzernen werden Beschäftigtendaten häufig bei einer zentralen Stelle gespeichert, z. B. bei der Muttergesellschaft, um eine einheitliche Personalverwaltung zu gewährleisten. Die Datenschutz-Grundverordnung geht nun erstmals auf diesen Bereich ein und hält fest, dass Unternehmensgruppen ein berechtigtes Interesse daran haben können, für interne Verwaltungszwecke Beschäftigtendaten zu übermitteln. In der Praxis wird hierdurch die Datenübermittlung erleichtert, ohne dass dabei der Schutz der Daten aus dem Auge verloren wird.

Datenübermittlung in die USA rechtssicher regeln

Die Übermittlung personenbezogener Daten wie Arbeitnehmerdaten in die USA ist für viele Unternehmen ein wesentlicher Baustein, um geschäftliche und personalpolitische Beziehungen sinnvoll gestalten zu können. Dafür benötigen die Betriebe rechtssichere Lösungen. Nach dem Wegfall der Safe-Harbor-Zertifizierung in Folge eines Urteils des Europäischen Gerichtshofs (6. Oktober 2015) hat die EU-Kommission mit dem „Privacy Shield“ eine Nachfolgeregelung vorgelegt. Der „Privacy Shield“ hat sich zu einer wichtigen Grundlage für die Datenübermittlung in die USA entwickelt. Er muss erhalten bleiben und auf der Grundlage von Praxiserfahrungen weiter ausgestaltet werden. Für mehr Rechtssicherheit ist es zudem unverzichtbar, dass Rechtsgrundlagen für die Datenübermittlung wie Standardvertragsklauseln und verbindliche Unternehmensregelungen erhalten werden. Die nationalen Datenschutzaufsichtsbehörden sind aufgefordert, sich übereinstimmend zu diesen Grundlagen zu bekennen.

Diensteanbieterschaft für Arbeitgeber beenden

E-Mail, Internet und Telefon wachsen zusammen. Die Nutzung solcher Kommunikationsmittel ist für die Unternehmen

unverzichtbar und entspricht den Interessen von Arbeitnehmern und Arbeitgebern. In Deutschland wird der Arbeitgeber allerdings nach vielfacher Auffassung „Diensteanbieter“ im Sinne des Telekommunikations- oder Telemediengesetzes, wenn er seinen Arbeitnehmern die private Nutzung von Internet und E-Mail erlaubt. Das zwingt Unternehmen – obwohl personalpolitisch nicht gewollt – zum Verbot der privaten Nutzung. Deshalb muss der nationale Gesetzgeber unabhängig von der Datenschutzgrundverordnung eine Klarstellung ins Auge fassen, die diese nicht nachvollziehbare Interpretation ausschließt. Ebenso muss klargestellt werden, dass der Arbeitgeber zur Aufrechterhaltung des ordnungsgemäßen Geschäftsbetriebs auch auf das betriebliche E-Mail-Fach des Arbeitnehmers Zugriff nehmen kann, um im Einzelfall den vereinbarungs- und gesetzmäßigen Gebrauch von Internet und E-Mail überprüfen zu können.

Kriminalitätsbekämpfung unterstützen

Unternehmen sind durch vielfältige internationale, aber auch nationale Regelungen verpflichtet, die Überprüfung gesetzlicher Vorschriften einzuhalten. Die Einhaltung von Gesetzen und die Überprüfung dieser Einhaltung (Compliance) stehen nicht im Widerspruch zum Datenschutz. Vielmehr ist Datenschutz ein Teil der Compliance. Dies setzt voraus, dass der Arbeitgeber Indizien für Regelverstöße nachgehen kann. Hierzu kann es im Einzelfall notwendig sein, bestehende Datenbestände präventiv gegeneinander abzugleichen oder auch ohne Kenntnis des Arbeitnehmers Daten zu erheben, zu nutzen und zu verarbeiten. Ebenso muss Hinweisen auf Regelverstöße effektiv nachgegangen werden können. Im Einzelfall kann zur Aufdeckung von Straftaten oder anderen schwerwiegenden Vertragsverletzungen eine gezielte Videoüberwachung notwendig werden. Ein solcher Einsatz von Videoanlagen wird von der Rechtsprechung zu Recht an strenge Voraussetzungen geknüpft. In diesem Umfang ist auch mit Geltung der Datenschutz-Grundverordnung der Einsatz aber auch unverzichtbar, um die Einhaltung von Recht und Gesetz zu gewährleisten.

Publikationen und Ansprechpartner

Beschäftigtendatenschutz vernünftig anpassen

Stellungnahme zum Gesetzentwurf zur Anpassung des Datenschutzrechts an die Datenschutz-Grundverordnung – Datenschutz-Anpassungs- und Umsetzungsgesetz EU, März 2017

Beschäftigtendatenschutz in Europa praxisnah ausgestalten

Stellungnahme zum Bericht des federführenden Ausschusses im Europäischen Parlament über die Datenschutzgrundverordnung, Dezember 2013

Europäischen Datenschutz angemessen aktualisieren

Stellungnahme zum Entwurf einer europäischen Datenschutzgrundverordnung, Juni 2012

Arbeitnehmerdatenschutz rechtssicher gestalten – Gesetzes- und Pflichtverstöße wirksam verhindern

Gemeinsame Stellungnahme mit dem BDI zum Entwurf

eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, Mai 2011

Datenschutz im Arbeitsverhältnis ausgewogen und rechtssicher gestalten

Positionspapier, Februar 2010

BDA | DIE ARBEITGEBER

Bundesvereinigung der Deutschen Arbeitgeberverbände

Arbeitsrecht

T +49 30 2033-1204

arbeitsrecht@arbeitgeber.de

Die jeweils neueste Ausgabe und weitere Hinweise zu diesem Thema finden Sie unter

www.arbeitgeber.de