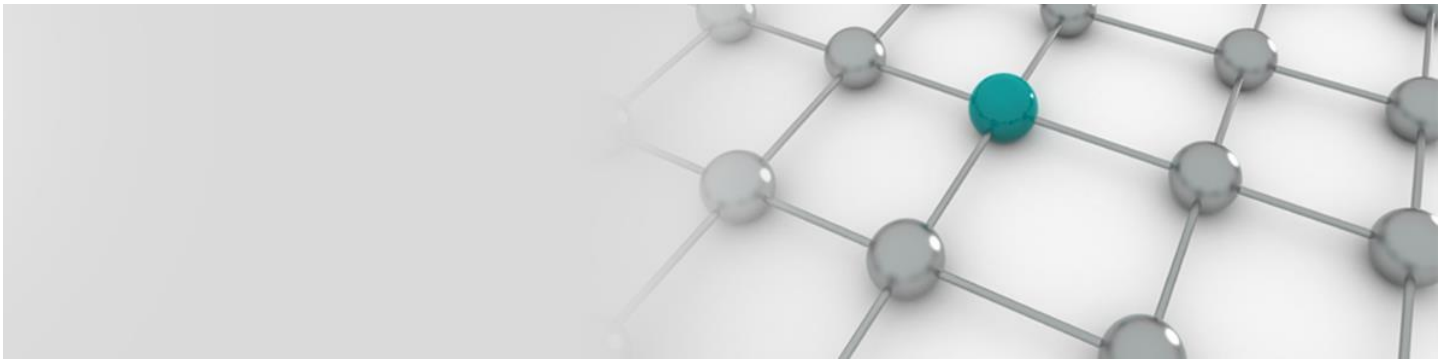

DATENSCHUTZ UND KONZERNPRIVILEG

Die „verantwortliche Stelle“…

Whitepaper

Datenschützer sowie der Gesetzgeber erteilen dem Konzernprivileg eine strikte Abfuhr.

AdOrga Solutions

Regina Mühlich
consulting@adorgasolutions.de

Inhalt

* Hinweis: Der Übersichtlichkeit wegen werden im Folgenden nur die männlichen Formen verwendet.

Befürworter von Erleichterungen in Konzernstrukturen fordern die Einführung eines Konzernprivilegs im Hinblick auf die datenschutzrechtlichen Bestimmungen. Datenschützer sowie der Gesetzgeber erteilen der damit einhergehenden Aufweichung des Datenschutzes jedoch eine strikte Abfuhr.

Seit September 2009 beinhaltet das BDSG einen speziellen gesetzlichen Erlaubnistatbestand für die Datenverwendung im Beschäftigtenverhältnis (§ 32 BDSG). Zentraler Erlaubnistatbestand für die Nutzung von personenbezogenen Geschäfts- und Kundendaten ist § 28 Abs. 1 Satz 1 BDSG.

1 Verantwortliche Stelle als Datenschutz-Adressat

„Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.“ (§ 3 Abs. 7 BDSG)

Das Bundesdatenschutzgesetz (BDSG) definiert, wer aus Datenschutzsicht „verantwortlich“ ist. Die Europäische Datenschutzrichtlinie stellt außerdem klar, dass die tatsächlichen objektiven Umstände bei der Feststellung des Verantwortlichen bedeutsam sind. Die verantwortliche Stelle ist diejenige Stelle, die „über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“ (Art. 2 d EU-DSRL).

Verantwortlich ist folglich das Unternehmen, welches die Entscheidungsgewalt innehat. Die datenschutzrechtliche Verantwortlichkeit ist relevant für die Feststellung, welche Stelle als Adressat einer Datenschutzfrage fungiert. Besondere Bedeutung kommt ihr im Zusammenhang mit spezifischen Anfragen der staatlichen Datenschutzkontrolle sowie der Betroffenen zu. An sie richten sich die Prüfungen der Datenschutzaufsicht, verbunden mit den Auskunfts- und Duldungspflichten.

Im Sanktionsfall ist die verantwortliche Stelle Adressat von Beanstandungen, Anordnungen, Untersagungsverfügungen oder Bußgeldern. Betroffene, also bestimmte oder bestimmbare Personen, zu denen „Einzelangaben über die persönlichen oder sachlichen Verhältnisse“ verarbeitet werden, können sich ebenso an die verantwortliche Stelle wenden. Auf diesem Wege können sie so die ihnen zustehenden Ansprüche nach Auskunft, Berichtigung, Sperrung, Löschung, Widerspruch sowie Schadenersatz (§ 34 BDSG Auskunft an den Betroffenen und § 35 BDSG Berichtigung, Löschung und Sperrung von Daten, § 7 BDSG Schadenersatz) geltend machen.

1.1 Kunden- und Geschäftsdaten

Gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist die Verwendung von personenbezogenen Kunden- und Geschäftsdaten zulässig, sofern dies für die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses notwendig ist. Das BDSG ermöglicht hiermit eine unter anderem konzernweite Datenverwendung zu Zwecken gegenüber Kunden. Dies betrifft z. B. IT—Services an denen Gruppenunternehmen beteiligt sind. Voraussetzung ist aber, dass dies dem Kunden bekannt ist (z. B. Leistungserbringung durch konzernweite Rechenzentren). Eine besondere Privilegierung von Konzernen erfolgt in diesem Zusammenhang aber nicht.

Die Verwendung von personenbezogenen Daten auf der Grundlage einer Einwilligung gemäß § 4a BDSG ist möglich.

1.2 Beschäftigtendaten

Die Verwendung von personenbezogenen Beschäftigtendaten ist zulässig sofern dies für die Begründung, Durchführung oder Beendigung des Beschäftigtenverhältnisses notwendig ist (§ 32 BDSG). Eine besondere Privilegierung von Konzernunternehmen ist hier ebenfalls nicht vorgesehen. Allerdings ermöglicht sie eine konzernweite Verwendung von Beschäftigtendaten in einer zentral geführten Personaldatenbank wenn z. B. ein ausdrücklicher Konzernbezug des Arbeitsverhältnisses im Arbeitsvertrag gegeben ist. Dies ist z. B. beim Einsatz des Arbeitnehmers bei verschiedenen Tochtergesellschaften der Fall.

Die konzernweite Verwendung von Beschäftigtendaten ist natürlich grundsätzlich zulässig, wenn eine ausdrückliche Einwilligung des Beschäftigten (§ 4a BDSG) vorliegt. Wobei umstritten ist, ob eine Einwilligung im Beschäftigtenverhältnis der gesetzlichen Anforderung aufgrund des bestehenden Über-/Unterordnungsverhältnisses zwischen Arbeitgeber und Beschäftigten „stets freiwillig“ entsprechen kann.

2 Konzernprivileg nicht mit Datenschutz vereinbar

Der **Grundansatz des Datenschutzrechts lehnt ein Konzernprivileg ab**, um Schutzlücken von Grund auf zu vermeiden. Würde, wie von einigen Befürwortern gefordert, das Prinzip des Konzernprivilegs datenschutzrechtliche Geltung erlangen, wären alle konzernierten Unternehmen als eine einzige verantwortliche Stelle im Sinne des Datenschutzrechts qualifiziert. Dies hätte zur Folge, dass der gesamte konzerninterne Datenverkehr als unternehmensinterner Datenverkehr gelten würde.

Der **Gesetzgeber hat sich jedoch deutlich gegen ein so geartetes Konzernprivileg entschieden**, das es erlauben würde, alle Konzerngesellschaften als eine einheitliche verantwortliche Stelle zu sehen.
Die wirtschaftliche Einheit begründet und erfordert hiernach nicht auch eine Informationseinheit. Sämtliche Konzernunternehmen stehen im datenschutzrechtlichen Verhältnis de facto als „Dritte“ zueinander. Adressat datenschutzrechtlicher Vorschriften ist und bleibt stets nur das einzelne Konzernunternehmen (einschließlich der Konzernmuttergesellschaft), nicht jedoch der Konzern selbst.

3 Weiterführende Informationen

Seitens Hessischen Datenschutzbeauftragten wurde durch die ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer“ am 11. Januar 2005 ein Arbeitsbericht erstellt.
Link zum Arbeitsbericht: https://www.datenschutz.hessen.de/ft-konzerndatenschutz.htm

4 Links und Gesetze

§ 3 BDSG http://www.gesetze-im-internet.de/bdsg_1990/__3.html
§ 4a BDSG http://www.gesetze-im-internet.de/bdsg_1990/__4a.html
§ 28 BDSG http://www.gesetze-im-internet.de/bdsg_1990/__28.html
§ 32 BDSG http://www.gesetze-im-internet.de/bdsg_1990/__32.html