Pest oder Lepra – ist der Betriebsrat „verantwortliche Stelle ?

Wie leicht man als BR mit einem einzigen Wort seine Identität aufs Spiel setzen kann

Von Kai Stumper

„Pest oder Lepra – was hätten Sie denn gern ?“ Man mag des Öfteren im Leben den Eindruck haben, vor diese Frage gestellt zu sein – aber im Datenschutzrecht ? Und als Betriebsrat ? Ja. Zumindest seitdem die DSGVO gilt. Denn seit diesem Zeitpunkt wird heftigst diskutiert, ob der Betriebsrat (BR) selbst eine verantwortliche Stelle ist. Und was sich zunächst ziemlich akademisch und praxisfern anhört, hat möglicherweise äußerst schmerzhafte Folgen für die BR-Arbeit. Aber der Reihe nach.

Was ist überhaupt eine „verantwortliche Stelle“ ? Nun, ganz einfach: das ist gem. Art. 4 Nr. 7 DSGVO die Instanz, die Daten verarbeitet. Und das ist nach bisherigem Verständnis der Arbeitgeber. Allerdings weiß jeder, dass ja auch im BR-Büro Daten verarbeitet werden. Zwar ist die Verarbeitung personenbezogener Daten vor dem Hintergrund des informationellen Selbstbestimmungsrechts aus Art. 1 I i.V.m. Art. 2 I GG „an sich“ verboten. Sie ist aber auch dem BR erlaubt, wenn er dafür eine Rechtsgrundlage findet. Zu solchen Rechtsgrundlagen gehören zunächst einmal Spezialgesetze wie eben das BetrVG. Wenn also der BR z.B. die Bewerbungsunterlagen von neu einzustellenden Mitarbeitern vom AG erhält, dann geschieht das aufgrund von § 99 BetrVG, der dies ausdrücklich im Falle von Einstellungen anordnet.

Aber zusätzlich darf der BR auch Daten verarbeiten, wenn es lediglich für die Erfüllung seiner Aufgaben „erforderlich“ ist. Ebenso, wie für den AG gilt nämlich § 26 BDSG auch für den BR, allerdings mit dem Unterschied, dass die Zweckrichtung der Erforderlichkeit sich beim AG am Arbeitsvertrag zu messen hat, beim BR „zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten“. Hierauf könnte sich also z.B. ein BR berufen, der während der Sprechstunde ein persönliches Gespräch mit einem Arbeitnehmer etwa über dessen Beschwerde fehlerhafter Lohnabrechnung führt und sich dabei Notizen auf dem Laptop macht. Er könnte allerdings hierfür auch dem betroffenen Arbeitnehmer ein Einwilligungsformular über den Tisch reichen und abzeichnen lassen.

Das BAG schützt den Betriebsrat

Warum ist also nicht auch der BR „verantwortliche Stelle“ ? Darüber könnte man lange sinnieren, gäbe es nicht das Bundearbeitsgericht (BAG), das in liebevoller Servicementalität dem BR einen Schutzschirm angeboten hat. Bisher.

Das BAG hat nämlich in mehreren Urteilen (zuletzt 14.1.2014 .- 1 ABR 54/12) erklärt, dass der BR schon deshalb keine verantwortliche Stelle sein könne, weil er im Gesetz keiner der dafür vorgesehenen Beschreibungen unterfalle. Mit „Gesetz“ meinte das BAG freilich das alte BDSG. Inzwischen gibt es ein „neues“ BDSG und eine DSGVO. Doch auch darin findet sich keine Beschreibung dessen, was den BR ausmacht. Es sei denn, man wollte sagen, dass die Formulierung „oder andere Stelle“ neben den natürlichen und den juristischen Personen Raum dafür gäbe, hier den BR einzuordnen. Und genau das tun inzwischen viele – wenn auch eher arbeitgeberorientierte – Autoren. Und sie stützen ihre Meinung gleich noch mit einem weiteren Joker: die DSGVO sei nämlich als unionsrechtliche Verordnung mit höherem Rang ausgestattet, als das Betriebsverfassungsgesetz (BetrVG).

Was soll nun das wieder, da besteht doch gar kein Zusammenhang ?
Doch, wenn man die bisherige Argumentation des BAG ansieht. Denn das BAG hat letztlich dem BR die Rolle als verantwortliche Stelle abgesprochen, um ihn zu schützen. Und ein solcher Schutz kommt nicht aus dem Datenschutzrecht, sondern aus dem BetrVG. Der BR habe eine Sonderrolle und sei als betriebsverfassungsrechtliches Organ eigener Art Teil der verantwortlichen Stelle, eben gerade weil er ein betriebsverfassungsrechtliches Ehrenamt ausübe.

BAG 18.07.2012 – 7 ABR 23/11:

„Die Betriebsräte - und damit auch der Gesamtbetriebsrat - unterliegen nicht der Kontrolle durch den betrieblichen Datenschutzbeauftragten nach § 36 Abs. 5 und § 37 BDSG. Ein Kontrollrecht des Datenschutzbeauftragten wäre mit der vom Betriebsverfassungsgesetz vorgeschriebenen Unabhängigkeit des Gesamtbetriebsrats von der Arbeitgeberin unvereinbar. Ein so massiver und wertungswidersprüchlicher Eingriff in ein Strukturprinzip des Betriebsverfassungsgesetzes kann dem Bundesdatenschutzgesetz nicht entnommen werden. Das Gesetz erweist sich insoweit als lückenhaft, als es keine Vorschriften über das Verhältnis der beiden Organe zueinander enthält.

(…)

bb) Die Ausübung der in § 36 Abs. 5 und § 37 BDSG vorgesehenen Kontrollrechte des Datenschutzbeauftragten gegenüber dem Gesamtbetriebsrat würde dessen gesetzlich vorgeschriebene Unabhängigkeit von der Arbeitgeberin beeinträchtigen. Die Kontrollmaßnahmen wären der Arbeitgeberin zuzurechnen. Zutreffend hat das Landesarbeitsgericht erkannt, daß der betriebliche Datenschutzbeauftragte keine "neutrale Stellung" zwischen Arbeitgeberin und Gesamtbetriebsrat einnimmt.

(1) Der Datenschutzbeauftragte wird nach § 36 Abs. 1 BDSG vom Arbeitgeber ausgewählt und bestellt. Der Bestellungsakt als solcher unterliegt nicht der Mitbestimmung des Betriebsrats. Der Betriebsrat hat auch kein Beteiligungsrecht, das es ihm - wie etwa bei der Bestellung und Abberufung angestellter Betriebsärzte oder Fachkräfte für Arbeitssicherheit nach § 9 Abs. 3 ASiG - ermöglichen würde dafür zu sorgen, daß das Amt von einer Person auch seines Vertrauens wahrgenommen wird.

(…)

Der Datenschutzbeauftragte erfüllt Aufgaben des Arbeitgebers, denn er hat nach § 37 Abs. 1 Satz 1 BDSG die Ausführung dieses Gesetzes im Unternehmen "sicherzustellen". Hierbei handelt es sich um eine Pflicht, die zunächst dem Unternehmen (Arbeitgeber) selbst als dem Normunterworfenen obliegt.“

Wo führt das eigentlich hin ?

Aber der Joker derjenigen, die nun doch den Br als verantwortliche Stelle i.S.d DSGVO sehen, besteht darin, darauf hinzuweisen, die DSGVO stünde ja nunmal über nationalem Recht, also über dem

BetrVG. Damit entfielen dann aber eben auch derartige Schutztendenzen.
Schutz ? Ja, aber wovor ? Was ist denn so dramatisch, wenn man einfach den BR „verantwortliche Stelle“ sein lässt ?
Tja – laut DSGVO ist die verantwortliche Stelle der Adressat aller im Gesetz festgelegten Pflichten; sie haftet. Und sie hat einen eigenen betrieblichen Datenschutzbeauftragten (bDSB) zu bestellen.

Wenn man sich das einmal vorstellt und zu Ende zu denken versucht, dann führt das dazu, dass man es irgendwie nicht zu Ende denken kann. Denn:

1. Wie soll der BR haften, ist er doch nicht rechtfähig und außerdem noch vermögenslos ?
2. Wer soll den Job des bDSB übernehmen – etwa derjenige, den der AG bereits hat ?
3. Muss der BR dann auch die Transparenzpflichten gem. Art. 13, 14 DSGVO einhalten und die Arbeitnehmer über die Verarbeitungsprozesse im BR-Büro informieren ?
4. Muss der BR dann auch ein eigenes Verzeichnis von Verarbeitungstätigkeiten (VVT) führen, wie es die Aufsichtsbehörden vom AG fordern können ?
5. Muss der BR Verträge mit Auftragsverarbeitern gem. Art. 28 DSGVO schließen ?

Verschärft gelebt, verschärft gehaftet ?

Allein die Frage 1 könnte bereits dazu führen, dass künftig (noch) weniger Arbeitnehmer Lust verspüren, sich als BR aufstellen zu lassen. Warum sollte man freiwillig in ein offenes Haftungsmesser laufen ? Warum also sollte man sich freiwillig die Pest holen, wenn man es auch einfach unterlassen kann, sich zum BR zu machen ?

Zumal die Haftungsmaßstäbe sich ja gerade durch die DSGVO drastisch verschärft haben und bis zu zehn bzw. zwanzig Mio. Euro laufen. Die Vorstellung, ein BR müsse solche Summen aufbringen, ist natürlich absurd. Aber selbst, wenn dieser Rahmen bei weitem nicht ausgeschöpft wird, was ja auch bei Unternehmen schon nicht üblich ist: woher sollte das Gremium auch nur 100 Euro nehmen, wenn es doch rechtlich gesehen nicht geschäftsfähig ist und noch nicht mal einen Cent besitzt ?

Eine Lösung wäre, dass jedes einzelne BR-Mitglied persönlich haftet. Das ließe sich für zivilrechtliche und sogar für strafrechtliche Haftungstatbestände formaljuristisch mit Ach und Krach irgendwie herleiten. Aber damit würde man zugleich die Schutzfunktion des BetrVG aushebeln, dass dem Betriebsratsamt die Funktion der Ehrenamtlichkeit und der Unentgeltlichkeit zuweist. Selbst die DSGVO tendiert in Erwägungsgrund 148 dazu, gegenüber natürlichen Personen anstelle einer Geldbuße eine Verwarnung genügen zu lassen.

Das funktioniert allerdings nicht, wenn eine vorsätzliche oder grob fahrlässige Haftung zur Debatte steht. In solchen Fällen wird es auch eng mit der Argumentation über das Ehrenamt.

Bliebe also nur eine andere Lösung, nämlich, dass der AG die Haftung für den BR übernimmt. Das tut er ja ansonsten gem. § 40 BetrVG auch, wenn die Ausgabe „erforderlich“ ist. Dabei könnte eine Versicherungslösung helfen, die derzeit aber nicht besteht. Der AG könnte die Versicherungsbeiträge übernehmen, sofern sich am Markt ein entsprechendes Versicherungsangebot etablieren sollte. Auch Versicherungen werden aber wohl kaum bereit sein, für Vorsatz einzutreten und bei grober Fahrlässigkeit saftige Gebühren einfordern. Denn selbst der AG könnte ja stets sagen, dass das Eintreten für Vorsatz und grobe Fahrlässigkeit nicht „erforderlich“ i.S.d. § 40 BetrVG seien.

Hinsichtlich der Haftung wird gern empfohlen, der BR möge doch eine BV mit dem AG abschließen und darin dann Details zur Haftungsübernahme regeln. Dies sei wegen Art. 88 DSGVO auch kein Problem, denn der sei eine Öffnungsklausel auch für kollektivrechtliche Regeln.

Doch – es gibt ein Problem: eine BV hat nämlich den Sinn und Zweck, Rechte von Arbeitnehmern zu regeln. Für das reine Verhältnis zwischen AG und BR ist eine Regelungsabrede zu wählen, denn die Arbeitnehmer haben mit Haftungsverteilungen zwischen den Betriebsparteien nichts zu tun. Eine Regelungsabrede ist aber gerade keine kollektivrechtliche Regelung und nimmt deshalb auch nicht an der Öffnung durch Art. 88 DSGVO teil. Sie kann daher auch nicht solche Haftungsaussagen modifizieren, die die DSGVO vorschreibt. Allerdings geht es darum auch gar nicht, wenn lediglich die Abfederung zumindest der zivilrechtlichen Haftung und nicht deren Zuordnungsgrundsätze modifiziert werden, etwa durch eine Versicherungslösung. Trotzdem bleiben hier viele Fragen offen, die Situation erscheint höchst unbefriedigend. Es bleibt ein sehr ungutes Gefühl, das nicht gerade motivierend wirken dürfte.

Praxistipp: Erklären Sie ihrem AG, dass sich für ihn durch die DSGVO nichts ändert: er hat auch bisher schon gehaftet und tut das einfach auch weiterhin. Das ist der Preis für die betriebsverfassungsrechtliche Unabhängigkeit des Gremiums gegenüber Zugriffen des AG – alles nichts Neues.

Der betriebliche Datenschutzbeauftrage ist nicht neutral !

Und Frage 2 ist auch nicht gerade beruhigend. Welcher BR sollte sich wohl dabei fühlen, wenn der bDSB des Arbeitgebers plötzlich im BR-Büro herumschnüffelt und sämtliche Datenverarbeitungsvorgänge des BR minutiös dokumentiert ?

Klar, laut Gesetz ist der bDSB weisungsfrei und hat sich neutral zu verhalten, zudem unterliegt er einer Schweigepflicht gem. Art. 38 V DSGVO i.V.m. §§ 38 II, 6 V S. 2 BDSG .

Aber wie naiv der Glaube an die Unabhängigkeit ist, zeigt sich bei beliebigen Blicken in die Praxis, in der bDSB vehement gegen diese und andere Grundsätze ihrer Arbeit verstoßen.

Typische Beispiele dafür sind:

- Der bDSB reicht dem BR einen von ihm ausgearbeiteten Vorschlag für eine Betriebsvereinbarung (BV) herein.
- Der bDSB sitzt bei Verhandlungen mit dem AG auf der AG-Bank.
- Der bDSB behauptet, er müsse (ggf. mit dem BR gemeinsam) die Datenflüsse des BR in einem Verfahrensverzeichnis (heute nach DSGVO korrekt: „Verzeichnis der Verfahrenstätigkeiten, VVT“) katalogisieren.
- Der bDSB taucht als Rechteadressat in einer BV auf, z.B., wenn er das Recht erhält, bei einem BEM-Verfahren mitzuwirken (was reines Betriebsverfassungs- bzw. Sozialrecht darstellt).
- Der bDSB ist Personalchef, IT-Abteilungsleiter oder Geschäftsführer

Wenn man sich diese und ähnliche Fälle in der Praxis ansieht, kann man daran zweifeln, ob der Gesetzgeber dem Datenschutz einen Gefallen getan hat, indem er die Instanz des bDSB geschaffen hat. Erschreckend oft erinnert insbesondere die Bezugnahme von AG auf „ihren“ bDSB an Zeiten, in

denen die Obrigkeit noch mit Pickelhauben durch die Gegend lief. Gib einer Person einen Titel und sie ist kompetent – das sollte eigentlich als überwunden gelten, ist es aber nicht.
Ein Mensch, der eine Woche lang ein Seminar besucht hat, um sich am Freitag ein Zertifikat mit der Bestätigung aushändigen zu lassen, nun sei er betrieblicher Datenschutzbeauftragter, hat weder von IT noch vom Datenschutzrecht einen Schimmer. Es genügt aber, um den gesetzlichen Status zu erringen.

Viel zu oft halten AG dem BR irgendwelche „Stellungnahmen“ von bDSB vor die Nase, in denen völlig substanzlos, also ohne jede nachvollziehbare Begründung, feierlich erklärt wird, dieses oder jenes System, sei „unbedenklich“. Schon die bloße Nachfrage eines externen Beraters, welche Ausbildung der Funktion des bDSB im konkreten Falle zugrunde liege, wird als Hochverrat verurteilt, der nach eigenen Erfahrungen schon zum Abbruch von Verhandlungen geführt hat.
Dabei hat es eine Selbstverständlichkeit seriösen Umgangs zu sein, dass jeder Beteiligte ohne Nachfrage transparent macht, warum er meint, im Spiel mitmischen zu können. Wer nichts zu verbergen hat, der muss jederzeit seine Qualifikation nachweisen können. Und das ist auch der einzige Weg, wie man denjenigen bDSB zu ihrem Recht verhelfen kann, die wirklich qualifiziert, bemüht und gut sind. Gleichwohl darf man immer daran erinnern, dass keine noch so liebevolle Ausbildung dazu befugt, sich die Qualifikation eines Anwalts mit zwei Staatsexamen oder eines IT-Experten mit Informatikstudium oder ähnlichem Ausbildungsgang anzumaßen, wenn sie nicht eben schon da ist, was ja bei einigen bDSB durchaus der Fall ist. Genau das muss aber auch hinterfragt werden dürfen.

Selbst, wenn also in einem Unternehmen keines der oben genannten Beispiele zutrifft und selbst, wenn man einen nachgewiesen kompetenten bDSB vor sich hat (was selten der Fall ist): der bDSB wird vom AG bezahlt. Daran zu glauben, dass er in Grenz- und Konfliktfällen gegenüber dem BR wirklich neutral bleibt, mutet geradezu religiös an. Daher scheint man sich als BR neben der Haftungs-Pest auch noch die Lepra zu holen, wenn man sich als Verantwortliche Stelle behandeln ließe und sich darauf einließe, dass der bDSB nun auch noch das BR-Büro unter seine Fittiche nimmt.

Gleichwohl gehen vermehrt Stimmen aus der Datenschutz-Szene davon aus, dass bereits seit Mai 2018 automatisch der bDSB auch für den BR zuständig sei und ihn zu kontrollieren habe.

Als Alternative wird teilweise vorgeschlagen, der BR möge aus seinen eigenen Reihen einen „Sonderbeauftragten“ benennen, der eine analoge Aufgabe übernehmen könnte. Bereits die Bezeichnung macht deutlich, dass es sich hier eben gerade nicht um einen bDSB handelt.

Die Bestellung eines Sonderbeauftragten macht daher gerade dann Sinn, wenn sich der BR auf den Standpunkt stellen möchte, dass er sich gerade nicht für eine verantwortliche Stelle hält.

Dieser scheinbare „Ritt auf der Rasierklinge“ zwischen zwei sich eigentlich ausschließenden Rechtspositionen ist aber sogar empfehlenswert. Er erfordert allerdings, dass man in seiner Kommunikation strengstens auf die Wortwahl achtet. Die Funktion muss sich nicht „Sonderbeauftragter“ nennen, aber sobald der BR das Wort „betrieblicher Datenschutzbeauftagter“ dafür wählt, kommt es zu heillosen Abgrenzungsproblemen.

Praxistipp: Benennen Sie einen „Sonderbeauftragten für den Datenschutz“ aus den Reihen des Gremiums. Machen Sie dem AG klar, dass Sie den Datenschutz im BR-Büro als heiligen Gral ansehen, der nicht zur Disposition steht. Machen Sie ihm auch klar, dass die neue Funktion Kosten verursacht,

die er gem. § 40 BetrVG zu tragen hat. Machen Sie ihm das schmackhaft, indem Sie ihm die Alternativen aufzeigen: ein externer Datenschutzbeauftragter nur für das Gremium kostet noch mehr Geld und einem Gremium ohne diese Funktion droht eine höhere Haftung, für er ebenfalls aufkommen müsste.

Verantwortung und Verantwortung – derselbe Begriff, aber zwei Welten

Unabhängig davon sei an dieser Stelle betont, dass niemand ernsthaft bestreitet, dass die Aufsichtsbehörde seit jeher auch den BR in vollem Umfang kontrollieren darf. Denn im Verhältnis zu ihr wirkt keine betriebsverfassungsrechtliche Privilegierung; die Aufsichtsbehörde hat staatliche Befugnisse und damit eine ganz andere Stellung, als ein bDSB.

Das ist auch kein Widerspruch zur Haltung, wonach der BR keine verantwortliche Stelle i.S.d. DSGVO sei. Schließlich hat das BAG hat schon vor Einführung der DSGVO die Ansicht vertreten, dass der BR „verantwortlich“ für seine Datenverarbeitung sei, auch ohne dass er deshalb „verantwortliche Stelle“ i.S.d. Datenschutzgesetze sei. So gesehen gibt es also, wie so oft in der Rechtssprache, zwei Begriffe, die gleich lauten, aber etwas unterschiedliches ausdrücken, hier also zwei Verantwortungsbegriffe.

BAG 12.08.09 – 7 ABR 15/08:

„(b) Werden dagegen auf dem Rechner des Betriebsrats personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbetriebliche Gestaltung nach der Anlage zu § 9 Satz 1 BDSG so zu organisieren, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in das Datenverarbeitungssystem eingegeben, verändert oder entfernt worden sind *(Nr. 5 der Anlage zu § 9 Satz 1 BDSG)*. Die Verantwortung dafür trägt aber der Betriebsrat, der die geeigneten und erforderlichen Sicherungen festzulegen hat. Als Teil der verantwortlichen Stelle iSv. § 3 Abs. 7 BDSG ist der Betriebsrat selbst dem Datenschutz verpflichtet und hat eigenständig über Maßnahmen zu beschließen, um den Anforderungen des BDSG Rechnung zu tragen *(vgl. BAG 12. August 2009 - 7 ABR 15/08 - Rn. 27 mwN, BAGE 131, 316)*. Aus der Eigenverantwortlichkeit des Betriebsrats folgt dessen Pflicht, ua. für die in Satz 2 Nr. 5 der Anlage zu § 9 Satz 1 BDSG vorgesehene Eingabekontrolle Sorge zu tragen und zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind. Die danach grundsätzlich gebotene individuelle Zugangsregelung zum gemeinsam genutzten Betriebsrats-PC setzt jedoch nicht zwingend einen für die Arbeitgeberin erkennbaren personalisierten Zugang zum PC voraus. Eine geeignete Eingabekontrolle lässt sich auch anders konfigurieren, etwa über Eingaben, deren persönliche Zuordnung nicht dem Arbeitgeber, sondern nur dem Betriebsrat bekannt ist *(zB durch die Bezeichnungen als BR 1, BR 2, BR 3 usw.)*.

(…)

3. Das Einsichtsrecht einzelner Mitglieder des Betriebsrats ist unabdingbar. Es kann weder durch die Geschäftsordnung noch durch einen Beschluss des Betriebsrats eingeschränkt werden *(Fitting BetrVG 24. Aufl. § 34 Rn. 33; GK-BetrVG/Raab 8. Aufl. § 34 Rn. 30; Richardi/Thüsing BetrVG 11. Aufl. § 34 Rn. 27)*.Es kommt danach nicht auf den Streit der Beteiligten an, ob der Betriebsrat das elektronische Einsichtsrecht nach § 34 Abs. 3 BetrVG überhaupt beschränkt hat und ob seine tatsächliche Handhabung auf einer Rechtsgrundlage beruht.“

Auch die oben angesprochenen Fragen 3. und 4. könnte ein BR unproblematisch darstellen, ohne auf die Position verzichten zu müssen, er sei keine verantwortliche Stelle. Mehr noch: er könnte damit sogar eine Art „Imagepflege“ als datenschutzrechtlich besonders aufmerksam und akribisch betreiben. Den Arbeitnehmer gegenüber könnte er damit Killerphrasen, wie sie manchmal von Arbeitgebern verwendet werden, entgegenwirken, wonach BR vom AG penibelsten Datenschutz einforderten, aber selbst in einem Saustall lebten. Hier wären also mit überschaubarem Aufwand

sogar positive Effekte vorstellbar.
Und zumindest gegenüber der Aufsichtsbehörde, die schon immer für die Kontrolle der BR-Datenverarbeitung zuständig war, ist es völlig unabhängig vom hier dargestellten Meinungsstreit sicherlich sinnvoll, sauber dazustehen und dies durch ein vernünftig strukturiertes VVT (Muster auf www.firstlex.de/service/br-downloads/) abzubilden.

Praxistipp: Erstellen Sie für die Arbeitnehmer, deren Daten Sie verarbeiten, ein Informationsblatt, indem Sie die typischen Verarbeitungsprozesse nach Datentypen, Zwecksetzung, Empfängern und Löschfristen beschreiben. Orientieren Sie sich dabei an Art. 13 und 14 DSGVO.

Erstellen Sie außerdem ein VVT und pflegen Sie es kontinuierlich. Prüfen Sie die darin benannten Löschfristen und überwachen Sie sich selbst daraufhin, ob diese Löschungen auch tatsächlich erfolgen.

Der eigene Arbeitgeber als Auftragsverarbeiter ?

Problematisch wäre auch eine Antwort auf die obige Frage 5.

Was ist z.B., wenn der AG für den BR dessen Daten auf einem eigenen System speichert ? Das ist ja sogar der Normalfall, denn die meisten BR sind mehr oder weniger an die Infrastruktur des AG angeschlossen. So werden üblicherweise etwa die Mails des BR im selben System abgelegt, wie alle anderen Mails auch. Wäre der BR selbst eine verantwortliche Stelle, so müsste er mit der anderen verantwortlichen Stelle, die seine Daten verwaltet, also mit dem AG, einen Vertrag über die Auftragsdienstleistung gem. Art. 28 DSGVO schließen. Und von solchen Verträgen müsste es eine ganze Menge geben.

All das zeigt, dass derartige Gedankengänge leicht ins Groteske abdriften. Das allein wäre zwar kein rechtlich akzeptabler Grund, sie abzulehnen. Denn grotesk erscheint im Datenschutzrecht vieles, je nach Perspektive. Aber es ist eben hier die Konsequenz aus einem schon im Ansatz falschen Gedanken. Der BR ist nunmal keine verantwortliche Stelle.

Heißer Tipp: eine Geschäftsordnung

Eine weitere Absicherung gegen Argwohn und Haftung, gleich, ob von Seiten des AG oder der Aufsichtsbehörde, ist ein „Vertrag mit sich selbst“ – eine Geschäftsordnung zum Thema Datenschutz.

Oben wurde bereits gesagt, dass es der falsche Weg wäre, mit dem AG BV abzuschließen. Und es wurde gesagt, dass eine Regelungsabrede formal das passendere Instrument wäre. Aber auch sie ist ein Vertrag mit dem AG. Und wenn man sich auf den Standpunkt stellt, dass der BR gerade keine verantwortliche Stelle sei, dann gibt es auch keinen Grund, mit ihm irgendwelche Verträge über eine Rechtsposition zu schließen, die man ja nun gerade nicht vertritt. Denn solche Verträge würden ja nur dann Sinn machen, wenn das Gremium zumindest auch sich selbst zu irgend etwas verpflichten wollte. Aber zu was ? Es gibt keinen Grund dafür. Ein BR ist nicht dem AG gegenüber verpflichtet, sondern dem Gesetz, der Belegschaft und der Aufsichtsbehörde gegenüber, sonst niemandem.

Wenn das Gremium also etwas festlegen will, was die Eigenschaft von Spielregeln im Umgang mit Arbeitnehmerdaten aufweist, dann bitte nicht gegenüber dem AG, sondern allenfalls sich selbst gegenüber. Das aber ist dann eine GO (Muster für eine mögliche Struktur unter www.firstlex.de/service/br-downloads/).

Und eine solche GO kann sich durchaus an der Struktur einer z.B. Rahmen-BV zur IT orientieren. Das gilt aber eben nur thematisch, nicht aber hinsichtlich der Verpflichtungsachse, also nicht hinsichtlich einer Unterwerfung unter den AG.

Eine Selbstverpflichtung in einer GO dürfte dagegen die Aufsichtsbehörde erfreuen. Sie macht deutlich, dass das Gremium das nötige Problembewusstsein hat und nicht herumdruckst, sondern aus eigener Initiative etwas tut, um den Stall sauber zu halten. Das senkt das Haftungsrisiko, soweit es überhaupt besteht (siehe dazu bereits oben) und es ist auch ein gutes Argument gegenüber dem AG und dessen bDSB, sich nicht vereinnahmen zu lassen, sondern im Gegenteil auf seine Eigenständigkeit und Eigenverantwortlichkeit zu bestehen.

Eine solche GO kann übrigens auch hervorragend mit dem oben skizzierten VVT verzahnt werden und damit ein ebenso professionelles Gesamtkonzept abbilden, wie es der AG tut, wenn er BV abschließt und diese mit seinen VVT verknüpft – wenn er es richtig macht.

Allerdings muss darauf geachtet werden, dass die GO nicht übers Ziel hinausschießt, indem sie bestimmten Gremiumsmitgliedern Sonderzugriffsrechte einräumt, andere aber leer ausgehen lässt. In bestimmten Fällen, wie etwa bei betrieblichen Eingliederungsmaßnahmen und den damit verbundenen Akten, besteht zwar ein solches Interesse. Dieses Interesse steht aber tendenziell in Widerspruch zu den Informationsrechten der Gremiumsmitglieder in Bezug auf das Gremium und seine Arbeit im Ganzen.

So sagt das BAG z.B. schon 1997 (11.11.1997, 1 ABR 21/97):

„§ 34 Abs. 3 BetrVG soll sicherstellen, dass sich jedes Betriebsratsmitglied ohne zeitliche Verzögerung über die Vorgänge im Betriebsrat informieren kann *(vgl. BT-Drucks. VI/2729 S. 23).* Durch den damit zum Ausdruck gebrachten Grundsatz der gleichen Informationsmöglichkeiten will das Gesetz ausschließen, dass Mitglieder aufgrund ihres Status oder aufgrund übertragener Sonderaufgaben *(zB als Vorsitzender oder dessen Stellvertreter, als Ausschussmitglied, Systemadministrator oder aufgrund einer Freistellung)* gegenüber Betriebsratsmitgliedern ohne besondere Funktionen über einen Informationsvorsprung verfügen. Deshalb ordnet das Gesetz ausdrücklich an, dass sich alle Betriebsratsmitglieder selbst dann einen Überblick über die Gesamttätigkeit des Betriebsrats verschaffen können, wenn der Betriebsrat von der Möglichkeit der Delegation von Aufgaben auf Ausschüsse Gebrauch macht. Es liegt in der Natur der Sache, dass Mitglieder, die nach § 38 BetrVG von ihrer beruflichen Tätigkeit freigestellt sind, durch die Kontinuität ihrer Arbeit im Betriebsrat regelmäßig über ein aktuelleres Wissen der betriebsratsrelevanten Themen verfügen. Umso deutlicher wird der Zweck des § 34 Abs. 3 BetrVG, dass alle übrigen Mitglieder des Betriebsrats zumindest die Möglichkeit haben müssen, sich „jederzeit“ zu informieren.“

Praxistipp: Erstellen eine Geschäftsordnung zum Thema Datenschutz und verzahnen Sie diese mit einem Verzeichnis der Verarbeitungstätigkeiten (VVT). Das wirkt haftungsreduzierend und hält den AG auf Distanz, der mit dem Argument an Ihre Tür klopft, Sie würden nicht genug für den Datenschutz tun und deshalb müsse er es nun tun.

Hüten Sie sich vor BV oder Regelungsabreden, in denen der AG Ihnen anträgt, datenschutzrechtliche Verpflichtungen einzugehen. Tun Sie das, so haben Sie damit bereits unausgesprochen akzeptiert, dass Sie sich als verantwortliche Stelle begreifen und damit ein Eigentor geschossen.

Welche Position soll man nun einnehmen ?

Am einfachsten bleibt schlicht eine Positionierung, die sich auf die bisherige Rechtssituation bezieht. Denn:

- Art. 4 Nr. 7 passt schon vom Wortlaut her nicht. Verantwortliche Stelle kann zwar auch „jede andere Stelle“ sein, die aber gem. Art 4 Nr. 7 DSGVO „über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet“. Genau das tut der BR aber nicht bzw. nur in geringfügigem Ausmaß. Denn die Zwecke, für die der BR Daten verarbeiten darf, sind durch das Gesetz vorgegeben. Wenn also z.B. der AG gem. § 99 BetrVG dem BR im Rahmen einer Einstellung die Bewerberunterlagen übermittelt, dann erhält der BR diese nicht, weil es ihm gerade so gefällt, sondern weil es seine betriebsverfassungsrechtliche Aufgabe ist.
  Auch und gerade die Mittel der Verarbeitung stellt der AG, nicht der BR.
  Daher lässt sich gut vertreten, dass der BR eben gerade nicht „verantwortliche Stelle“ ist.
- Bis heute gibt es weder eine Gerichtsentscheidung, die vom bisherigen allgemeinen Standpunkt zur Frage der Verantwortlichkeit abweicht, noch haben die Aufsichtsbehörden hierzu eine Position bezogen, die als Richtungsänderung betrachtet werden könnte.
- Um die vielfältigen Fragezeichen zu beantworten, die oben skizziert wurden, wäre eine gesetzliche Initiative erforderlich. Diese ist bis jetzt aber nicht ersichtlich. In der Zwischenzeit sollte man sich nicht nervös machen lassen. Insbesondere ist dringend davon abzuraten, ohne jede Not BV zu verabschieden, die das Kontroll- und Haftungsgefüge zwischen AG, bDSB und BR zum Nachteil des BR verschieben.

Praxistipp: Machen Sie dem AG klar, dass Sie sich nicht als verantwortliche Stelle i.S.d. Art. 4 Nr. 7 DSGVO betrachten, weil der dortige Tatbestand schon vom Wortlaut her nicht passt (s.o.). Außerdem fehlt es an gesetzlichen Regelungen und Gerichtsentscheidungen, um eine andere Position begründen zu können.

Es ist also (zumindest noch) nicht nötig, sich zwischen Pest und Lepra zu entscheiden oder sich gar beides gleichzeitig aufzuhalsen. Der einfachste Weg ist, weiterhin an der bisherigen Rechtssituation festzuhalten. Denn dafür gibt es nach wie vor gute Argumente.

Zugleich kann man aber aus Gründen der Transparenz und im Hinblick auf die Überwachungsfunktion der Aufsichtsbehörde freiwillig einige Schritte unternehmen, um sich selbst und der Belegschaft zu beweisen, dass das Gremium datenschutzrechtlich sauber ist. Auch das gehört zum Ehrenamt.

****

Dr. Kai Stumper

Rechtsanwalt, Datenschutzbeauftragter, Seminarreferent und Fachbuchautor, ist bundesweit für Betriebs- und Personalräte tätig.

www.firstlex.de

www.firstdigi.de