

DATENSCHUTZ- BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Chefredakteur: Dr. Carlo Piltz

Schriftleitung: Prof. Dr. Alexander Golland, Tilman Herbrich, Philipp Quiel, Laurenz Strassemeyer

Editorial

Prof. Dr. Alexander Golland

Zurück in die Zukunft (Limited German Edition)

Seite 197

Stichwort des Monats

Stephan Hansen-Oest

Ist Art. 32 DSGVO dispositiv?

Seite 198

Datenschutz im Fokus

Dr. Tobias Rothkegel und Dr. Konrad Lang

NIS2: Vernachlässigbare Geschäftstätigkeiten nach § 28 Abs. 3 BSI-Gesetz

Seite 204

Dr. Carlo Piltz und Ilia Kukin

Datenschutzrechtliche Aspekte der Betriebsratswahl

Seite 208

Christian Aretz

Die Illusion des Nachweises

Seite 211

Dr. Arne Brest

Art. 15 DSGVO: Was ist im Kündigungsschutzverfahren herauszugeben?

Seite 216

Wiebke Reuter und Dr. Julius Alexander Remmers

Datenpannen melden im Wandel: Was das Digital Omnibus-Paket für Art. 33 DSGVO bedeutet

Seite 218

Dr. Maximilian Leicht

Cyber Resilience Act – Impulse für Datenschutzcompliance aus dem IT-Sicherheitsrecht

Seite 223

Aktuelles aus den Aufsichtsbehörden

Anna-Lena Eswein

Neue Anforderungen an den Kinderdatenschutz – Praxisfolgen aktueller Behördenpositionen

Seite 226

Dr. Maximilian Wagner

Datenschutz in der wissenschaftlichen Forschung

Seite 230

Rechtsprechung

Rudi Kramer

Haftung des Auftraggebers für Mitarbeiterexzess beim Auftragsverarbeiter

Seite 234

Dr. Dominik Sorber und Dr. Christina Knoepffler

Wissen ist Macht (und Geld) – Auskunftsanspruch über Gehaltsinformationen bei einer Personalvermittlung

Seite 238

Thies Schmitte und Tim Wybitul

KG: Verbandsklage auf immateriellen DSGVO-Schadenersatz unzulässig

Seite 240

Marcus Beckmann

Kein datenschutzrechtliches Beweisverwertungsverbot: Rechtsgrundlagen können nebeneinander gelten

Seite 243

Tilman Herbrich und Dr. Nico Bilski

Teilweise Niederlage für TikTok: Kein Drittlandtransfer ohne Nachweis des angemessenen Schutzniveaus

Seite 247

Service

Ilia Kukin

Schild/Horlbeck – Der Datenschutzverstoß

Seite 251

■ **Nachrichten** Seite 202

Datenschutzrechtliche Aspekte der Betriebsratswahl

Die Vorbereitung der Betriebsratswahl ist datenschutzrechtlich anspruchsvoll. Für Arbeitgeber stellt sich vor allem die Frage, wer verantwortlich ist und wer welche Aufgaben übernimmt. Hinzu kommt, dass Wahlvorstände häufig eine eigene IT-Infrastruktur verlangen: getrennte Laufwerke, selbst kontrollierte Verschlüsselung, den Ausschluss administrativer Zugriffe durch die Unternehmens-IT. Weder die DSGVO noch das BetrVG setzen jedoch eine vollständig isolierte IT-Welt voraus, sondern ein angemessenes und dokumentiertes Schutzniveau. Der Beitrag ordnet die Verantwortlichkeiten, fasst Rechtsprechung und Aufsichtspraxis zusammen und zeigt, wie Arbeitgeber und Wahlvorstand die Wahl rechtssicher gestalten können.

I. Die datenschutzrechtliche Stellung von Betriebsrat und Wahlvorstand

Bei der Betriebsratswahl werden zahlreiche personenbezogene Daten verarbeitet: Wählerlisten, Unterstützungsunterschriften, Schriftverkehr mit Gewerkschaften und Kanzleien, interne Beratungsunterlagen. Wer dafür verantwortlich ist, war jahrelang umstritten. Mit § 79a BetrVG hat der Gesetzgeber die Diskussion geordnet.

Nach § 79a Satz 2 BetrVG bleibt der Arbeitgeber Verantwortlicher im Sinne der DSGVO. Zugleich muss der Betriebsrat die Datenschutzvorschriften eigenständig einhalten. Damit hat er eine gewisse „Hybridstellung“. Für den Wahlvorstand trifft § 79a BetrVG keine ausdrückliche Regelung. Dies ist allerdings kein Fall der bewussten Nichtregelung, sondern dürfte nach zutreffender Ansicht eine klassische Regelungslücke darstellen, die durch die analoge Anwendung des § 79a BetrVG auch auf den Wahlvorstand zu schließen ist (Sorber, DSB 2024, 239).

Das führt zu einer datenschutzrechtlich ungewöhnlichen Konstruktion: Der Arbeitgeber bleibt datenschutzrechtlich verantwortlich, während der Wahlvorstand organisatorisch unabhängig handelt und die erforderlichen technischen und organisatorischen Maßnahmen selbst umsetzen muss. Fachliche Weisungen darf der Arbeitgeber ihm dabei grundsätzlich nicht erteilen.

II. Welche Daten werden vom Wahlvorstand verarbeitet?

Die datenschutzrechtlichen Pflichten treffen den Wahlvorstand unabhängig davon, welche Daten er im Einzelnen verarbeitet. Art und Sensibilität der Daten bestimmen aber, welches Schutzniveau angemessen ist – die DSGVO folgt insoweit einem risikobasierten Ansatz. Daher lohnt sich ein Blick auf die typischerweise vom Wahlvorstand verarbeiteten Daten.

Die Datenverarbeitungen richten sich nach den einschlägigen Vorschriften über die Durchführung von Betriebsratswahlen (insb. § 2 WO) und den allgemeinen Vorschriften des BetrVG (insb. §§ 7 und 8 BetrVG). Die Rechts-

grundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. c DSGVO i.V.m. der jeweiligen Vorschrift aus dem BetrVG oder der WO. Bei besonderen Kategorien personenbezogener Daten (etwa bei Rückschlüssen auf die Gewerkschaftszugehörigkeit oder den Gesundheitszustand) greift der Ausnahmetatbestand des Art. 9 Abs. 2 lit. b DSGVO. Schon bei der Datenerhebung muss der Wahlvorstand den Datenschutz mitdenken und nur für die Durchführung der Wahl tatsächlich erforderliche Daten verarbeiten.

Besondere Aufmerksamkeit verlangt die Veröffentlichung von Wähler- und Vorschlagslisten. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg unterscheidet klar: Die Wählerliste muss zwar Geburtsdaten enthalten (§ 2 Abs. 1 WO), der öffentlich ausgelegte Abdruck darf sie hingegen nicht ausweisen, da § 2 Abs. 4 Satz 1 WO die Auslegung ohne Angabe der Geburtsdaten vorsieht und es für eine Veröffentlichung daher an einer Rechtsgrundlage fehlen würde (LfDI Baden-Württemberg, Verarbeitung des Geburtsdatums im Zusammenhang mit der Betriebsratswahl, 2026). Arbeitgeber und Wahlvorstand sollten diesen Unterschied sorgfältig beachten.

III. Pflichten des Wahlvorstands

Der Sensibilität der verarbeiteten Daten muss der Wahlvorstand ausreichend Rechnung tragen. Nach § 79a Satz 1 BetrVG analog ist er verpflichtet, bei der Verarbeitung aller Daten den Datenschutz eigenverantwortlich einzuhalten. Das BAG hat klargestellt, dass § 79a Satz 2 BetrVG (also die Verantwortlichkeit des Arbeitgebers) den Betriebsrat nicht von der Pflicht entbindet, das durch die Vorschriften der DSGVO verlangte Schutzniveau zu gewährleisten (BAG, Beschl. v. 9.5.2023 – 1 ABR 14/22). Dazu zählen neben der Einhaltung der Datenschutzgrundsätze nach Art. 5 Abs. 1 DSGVO, etwa der bereits angesprochenen Datenminimierung, auch die Implementierung geeigneter technischer und organisatorischer Maßnahmen wie Zugriffsbeschränkungen und Passwortschutz, sichere Aufbewahrung der Unterlagen, ein Löschkonzept sowie sichere Kommunikationswege. Für technische und organisatorische Maßnahmen bleiben die allgemeinen Vorgaben der Art. 24 und 32

DSGVO der Maßstab. Die Datenverarbeitung des Wahlvorstands unterliegt also denselben Schranken wie diejenige des Arbeitgebers.

Im Ergebnis ist zu empfehlen, dass der Wahlvorstand in Zusammenarbeit mit dem Arbeitgeber ein Datenschutzkonzept für die Wahl ausarbeitet, das sämtliche gesetzlichen Anforderungen abdeckt. Dies dient dann auch der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO. Dort ist insbesondere zu regeln, welche Schutzmaßnahmen der Arbeitgeber und welche der Wahlvorstand ergreift, welche Datenschutzpflichten der Wahlvorstand eigenständig erfüllt und wie mit Sicherheitsvorfällen und Betroffenenanfragen umgegangen wird. Darüber hinaus erfordert die Hybridstellung, dass der Wahlvorstand dem Arbeitgeber die zur Erfüllung seiner Pflichten erforderlichen Informationen bereitstellt. Sie müssen dem Arbeitgeber ermöglichen, die Datenschutzhinweise für Mitarbeiter sowie das Verzeichnis von Verarbeitungstätigkeiten entsprechend zu ergänzen, und daher alle erforderlichen Angaben enthalten. Gelangt der Arbeitgeber zum Ergebnis, dass eine Datenschutz-Folgenabschätzung erforderlich ist, muss der Wahlvorstand auch alle hierzu erforderlichen Informationen zuliefern. Nachdem der Betriebsrat gewählt ist, empfiehlt es sich, die Zusammenarbeit im Bereich des Datenschutzes in einer Betriebsvereinbarung zu regeln.

IV. Eigene IT für den Wahlvorstand?

Als Teil ihrer Tätigkeit und damit auch des Datenschutzkonzepts verlangen Wahlvorstände nicht selten eine eigene IT-Infrastruktur. Insbesondere eigene Hardware, getrennte Laufwerke und eigene Mailpostfächer (ggf. auch bei einem anderen Hoster) sind dabei oft Teil der Forderung. Der Impuls ist nachvollziehbar, da auf diese Weise sichergestellt werden kann, dass der Arbeitgeber auf die Daten des Wahlvorstands nicht einmal eine theoretische Zugriffsmöglichkeit hat.

Die Aufsichtsbehörden halten die Sorge der Wahlvorstände und Betriebsräte für nachvollziehbar. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) weist darauf hin, dass Administratorenrechte die Vertraulichkeit von Betriebsratsdaten gefährden können, und empfiehlt vor allem eine vom Betriebsrat (bzw. in der Wahlphase vom Wahlvorstand) kontrollierte Verschlüsselung (HmbBfDI, Tätigkeitsbericht 2023, S. 44). Unter Verweis auf die Auffassung in der Literatur stellt der HmbBfDI zudem fest, dass sogar ein Anspruch des Betriebsrats gegen den Arbeitgeber auf Zurverfügungstellung oder Finanzierung einer Verschlüsselungssoftware bestehen kann. Ob solche Maßnahmen des Wahlvorstands von der Kostentragungspflicht des Arbeitgebers nach § 20 Abs. 3 BetrVG gedeckt sind (im Kontext der laufenden Betriebstätigkeit sind die Vorgaben des § 40 Abs. 2 BetrVG einschlägig), ist eine rein arbeitsrechtliche Frage, deren Be-

antwortung von dem konkreten Konzept und den bereits bestehenden IT-Systemen im Unternehmen abhängt. Trotz dieser recht betriebsratsfreundlichen Aussage hält der HmbBfDI fest, dass eine vom Betriebsrat kontrollierte Verschlüsselung zwar vorzugswürdig, aber nicht in jedem Fall zwingend erforderlich ist. Gleiches gilt für eine vollständig getrennte IT-Infrastruktur. Entscheidend ist, ob die gewählte Lösung insgesamt ein angemessenes Schutzniveau erreicht und ausschließlich datenschutzkonforme Verfahren und Systeme eingesetzt werden.

Die Frage, wer die IT-Infrastruktur bereitstellt, ist für die datenschutzrechtliche Rollenverteilung aufgrund der Regelung in § 79a Satz 2 BetrVG unerheblich. Der Verantwortliche bleibt in jedem Fall der Arbeitgeber, und der Wahlvorstand ist nur verpflichtet, die IT-Lösungen so auszuwählen, dass sie den Anforderungen des Art. 32 DSGVO genügen. Nicht ausgewählt werden dürfen auch solche (IT-)Dienstleister, mit denen der Arbeitgeber aufgrund der Vorgaben des Art. 28 Abs. 1 DSGVO keinen Auftragsverarbeitungsvertrag schließen kann – also etwa Dienstleister, die keine Nachweise und Gewähr für die Einhaltung der DSGVO-Vorgaben bieten.

V. Die Rolle des Datenschutzbeauftragten

Neben der technischen Ausgestaltung stellt sich die Frage nach der Rolle des Datenschutzbeauftragten. Manchmal lehnen es Wahlvorstände ab, ihn einzubinden, vor allem aus Sorge vor Einblicken in interne Beratungen. Sie ordnen ihn dem Lager des Arbeitgebers zu, obwohl er seine Aufgaben nach Art. 38 Abs. 3 Satz 1 DSGVO weisungsfrei wahrnimmt.

§ 79a Satz 4 BetrVG enthält dazu eine Sonderregelung: Der Datenschutzbeauftragte ist zur Verschwiegenheit verpflichtet, soweit Informationen Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen. Darüber hinaus ist anerkannt, dass der Datenschutzbeauftragte auch für die Datenverarbeitungen des Betriebsrats (und damit auch des Wahlvorstands) zuständig ist (LfD Niedersachsen, FAQ Datenschutzrechtliche Position von Betriebsräten).

Insbesondere im Kontext von Betroffenenanfragen ist die Mitwirkung des Datenschutzbeauftragten eine von Aufsichtsbehörden akzeptierte Lösung (BayLDA, Tätigkeitsbericht 2024, S. 51). Will der Wahlvorstand aus Gründen der Vertraulichkeit die Daten (beispielsweise Kopien von Dokumenten) nicht an den Arbeitgeber herausgeben, kann die Beantwortung der Auskunftsanfrage durch den Datenschutzbeauftragten erfolgen, der die Teilauskünfte zusammenführt.

Der Datenschutzbeauftragte darf und sollte daher bei der Ausarbeitung des Datenschutzkonzepts und in der laufen-

den Tätigkeit des Wahlvorstands bzw. des Betriebsrats eingebunden werden. Aufgrund seiner unabhängigen Stellung kann er sogar als Vermittler zwischen Wahlvorstand und Arbeitgeber agieren, was häufig schneller und kosteneffizienter zu einvernehmlichen Lösungen führt als die Einschaltung externer Berater. Die inhaltliche Arbeit des Wahlvorstands bleibt dabei rechtlich geschützt.

VI. Was muss der Arbeitgeber gewährleisten?

Der Arbeitgeber muss in seiner Eigenschaft als datenschutzrechtlich Verantwortlicher sicherstellen, dass alle Vorgaben der DSGVO eingehalten werden. Da er aber nur sehr beschränkte Einflussmöglichkeiten auf die datenverarbeitenden Tätigkeiten des Wahlvorstands hat, muss er insoweit geeignete Rahmenbedingungen schaffen. In der Praxis bedeutet das eine enge Abstimmung mit dem Wahlvorstand zu mindestens folgenden Punkten:

1. Zugriffs- und Berechtigungskonzept,
2. Technische Schutzmaßnahmen,
3. Löschkonzept,
4. Gegenseitige Unterstützung und Dokumentation.

Wenn der Wahlvorstand keine eigene IT-Infrastruktur erhält, ist ein vollständiger technischer Ausschluss aller Administratorenrechte praktisch kaum erreichbar. Empfehlenswert sind dann Maßnahmen wie:

- Protokollierung administrativer Zugriffe,
- Vier-Augen-Prinzip,
- dokumentierte Ausnahmeprozesse,
- gesonderte Vertraulichkeitsverpflichtungen der IT,
- Information des Wahlvorstands vor notwendigen Zugriffen.

Mit dem Wahlvorstand sollte ferner abgestimmt werden, dass die Berechtigungen intern nach dem Need-to-know-Prinzip vergeben werden. Mit Blick auf die technischen Schutzmaßnahmen sind insbesondere Verschlüsselung, Multi-Faktor-Authentifizierung und separate Speicherbereiche zu empfehlen.

Ferner muss ein Löschkonzept abgestimmt werden. Wahlunterlagen dürfen nicht unbegrenzt gespeichert werden. Für die Wahlakten ist § 19 WO einschlägig, der die Aufbewahrung bis zur Beendigung der Amtszeit des Betriebsrats vorschreibt. Der Wahlvorstand sollte festlegen, welche Daten gespeichert werden, wie lange das erforderlich ist, wann gelöscht wird und wie Datenträger sicher vernichtet werden.

Die gegenseitige Unterstützung ist vor dem Hintergrund der Haftungsrisiken aus Arbeitgebersicht essenziell. Denn § 79a BetrVG privilegiert durch die Regelung der Verantwortlichkeit die Wahlvorstandsmitglieder dahingehend, dass sich der Anspruch aus Art. 82 Abs. 1 DSGVO gegen den Arbeitgeber und nicht gegen einzelne Mitglieder des

Wahlvorstands richtet (ArbG Bonn, Urt. v. 20.11.2024 – 5 Ca 663/24). Der Arbeitgeber wird in der Regel auch Adressat aufsichtsbehördlicher Maßnahmen sein. Etwas anderes gilt nur im Fall eines (Kollektiv-)Exzesses, also wenn ein oder mehrere Mitglieder des Wahlvorstands außerhalb ihrer Amtswahrnehmung handeln.

VII. Fazit

Die Datenschutzanforderungen bei Betriebsratswahlen werden in der Praxis oft unterschätzt. § 79a BetrVG hat die datenschutzrechtliche Rollenverteilung geklärt, ohne sie zu vereinfachen: Der Arbeitgeber bleibt Verantwortlicher, während Betriebsrat und (analog) Wahlvorstand den Datenschutz eigenverantwortlich umsetzen müssen. Diese Hybridstellung verlangt von beiden Seiten weniger ein Gegeneinander, sondern eine geordnete Zusammenarbeit.

Für die Praxis lassen sich drei Leitlinien festhalten. Erstens trägt der Arbeitgeber die Verantwortung, ohne den Wahlvorstand fachlich steuern zu dürfen. Statt Weisungen zu erteilen, muss er daher Rahmenbedingungen für die Durchführung der Wahl schaffen. Zweitens ist die Frage der eigenen IT keine des Datenschutzrechts, sondern vor allem der arbeitsrechtlichen Kostentragung. Entscheidend ist dabei auch nicht die Trennung der Infrastruktur, sondern ihre datenschutzkonforme Ausgestaltung. Drittens ist der Datenschutzbeauftragte trotz mancher Vorbehalte kein Gegner der Vertraulichkeit, sondern (abgesichert durch § 79a Satz 4 BetrVG) ein naheliegender Vermittler.

Wer diese Punkte frühzeitig abstimmt und die Zusammenarbeit später idealerweise in einer Betriebsvereinbarung verankert, reduziert Haftungsrisiken und vermeidet, dass Datenschutzfragen die Wahl selbst und die zukünftige Zusammenarbeit mit dem Betriebsrat belasten.

Autoren: Dr. Carlo Piltz ist Rechtsanwalt bei Piltz Legal in Berlin und spezialisiert im nationalen und internationalen Datenschutzrecht.



Ilia Kukin ist Rechtsanwalt und Associate bei Piltz Legal in Berlin.

