Workshop: **Datenschutzkultur im Betrieb – Beispiele für bewährte Regelungen und Erfahrungen aus der Praxis**

Eva Angerler, GPA-djp, Arbeit und Technik und Tom Gödel, BRVS IBM

Unter **Datenschutzkultur** verstehen wir die Art und Weise, wie im Betrieb mit dem Thema Datenschutz umgegangen wird. Folgende Fragen sind in diesem Zusammenhang relevant:

- Inwieweit sind die Betriebsräte, das Management, die Beschäftigten für Datenschutz sensibilisiert?
- Gibt es ein gemeinsames Verständnis, wie die DS-Grundsätze in Hinblick auf AN-Daten gelebt werden?
- Bekommt der BR jene Infos, die er für die Mitbestimmung an der Verwendung von personenbezogenen AN-Daten braucht?
- Gibt es eine regelmäßige Zusammenarbeit zum Thema AN-DS (Vereinbarter Prozess, DS-Kommission)?
- Wie wird mit (Interessen)-Konflikten umgegangen?

Entscheidend ist, wie die DS-Kultur tatsächlich gelebt wird. Rahmenregelungen sind wichtig, um eine gute Datenschutzkultur nachhaltig umzusetzen.

Input Eva:

Was muss eine DS-BV nach der DSGVO enthalten? (BV-Checkliste)

Unser Regelungsansatz für die betriebliche Praxis: Rahmen-BV und Systemanhänge (Rahmen-Muster-BV)

<u>Überblick über die Themenkomplexe, die die Muster-Rahmen-BV behandelt:</u>

- DS-Grundsätze, Datenkategorisierung
- Vorgangsweise bei Missbrauchsverdacht, Umgang mit Protokolldaten
- Interne DS-Kommission, Mitbestimmungskultur, -maßnahmen
- Vorgangsweise bei Auftragsdatenverarbeitung, Helpdesk, Fernwartung, mobile Nutzung;
- Informationspflichten des Unternehmens, Rechte des Betriebsrates
- Betroffenenrechte, Privatnutzung

<u>Folgende Materialien stehen zur Verfügung:</u>

- Checkliste für BVs nach der DSGVO
- Muster-Rahmenbetriebsvereinbarung zu Datenschutz

Input Tom

Datenschutzkultur Praxis – Tom bringt seine Erfahrungen dazu im Workshop ein.

Übungsteil:

Übung 1: „Wo stehe ich?“ nach Checkliste von Tom

Übung 2 „Regelungsvorschläge in Muster-BV durchsehen“ (Selbststudium Rahmen-BV – Themenkomplexe suchen und durchlesen und diskutieren, ob verständlich? Fragen? Erfahrungen dazu aus der betrieblichen Praxis?)

In der Arbeitsgruppe werden Fragen wie folgt behandelt: „Welche BVs haben wir? Wer hat Erfahrungen mit Verhandeln von Rahmen-BV? Wie schaut die Mitbestimmungskultur bei uns aus? Welche KooperationspartnerInnen habe ich?

Einige TeilnehmerInnen der Arbeitsgruppe verfügen über eine langjährig gewachsene Mitbestimmungskultur im Datenschutzbereich, während andere große Schwierigkeiten haben, zu den nötigen Informationen zu kommen und eine Rahmenbetriebsvereinbarung abzuschließen. Einige berichten, dass die Arbeitgeber Betriebsvereinbarungen wollen, die eine Blankozustimmung zu neuen IT-Systemen enthält. Das ist natürlich abzulehnen, und auch rechtlich gar nicht zulässig. Der Austausch über Strategien und Tipps in der Arbeitsgruppe ist sehr intensiv.

Checkliste für Betriebsvereinbarungen nach der EU-Datenschutzgrundverordnung (gilt ab dem 25.5.2018)

Bestehende und neue Betriebsvereinbarungen müssen im Einklang mit der DSGVO stehen. Widersprechen Regelungen in bestehenden Betriebsvereinbarungen diesen Grundsätzen, so werden sie in diesem Bereich ungültig. Die betroffene Betriebsvereinbarung insgesamt bleibt weiterhin in Geltung (bestehen).

Die folgende Checkliste[1] enthält zentrale Grundsätze der DSGVO, die in der Betriebsvereinbarung wie folgt abzubilden sind:

☑	Es ist eine **Differenzierung nach Datenarten/-kategorien** vorzunehmen (Art 9, 10): Einhaltung der erhöhten Schutzanforderungen für die Verarbeitung besonderer Datenkategorien (ethnische Herkunft, politische Meinung, Religion, sexuelle Orientierung, Gewerkschaftszugehörigkeit, genetische oder biometrische Daten, Daten über Verurteilungen und Straftaten).
☑	**Personenbezogene Daten** müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Art 5 Abs 1a). Die Regelungen zum Umgang mit ihren Daten müssen für Arbeitnehmer daher transparent und nachvollziehbar sein.
☑	**Zweckbindung** ist an- und auszuführen: Personenbezogene Daten dürfen nur für genau festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden. Es sind detaillierte Beschreibungen der Zwecke der geplanten Datenverarbeitung aufzunehmen. Diese können die betrieblichen Sozialpartner im Rahmen von Anhängen zur Betriebsvereinbarung ausführen. Eine Verarbeitung zu anderen Zwecken ist grundsätzlich unzulässig. Es ist davon auszugehen, dass zu unbestimmte und allgemeine Aussagen zu den zulässigen Zwecken oder die Angabe von Zweckbündeln von den Gerichten in Zukunft als unzulässig bewertet werden (Art 5 Abs 1 lit b).
☑	**Datenminimierung und Datensparsamkeit:** Die Datenerhebung und -verarbeitung muss auf das für die Zwecke der Datenverarbeitung notwendige Mindestmaß beschränkt sein (Art 5 Abs 1 lit c). Bereits bei Planung und Einführung der IT-Systeme sind Maßnahmen zur Umsetzung der Datenschutzgrundsätze in dem jeweiligen technischen System anzuführen. Dazu sieht die DSGVO die Modelle „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy by Design and by Default)" vor, zB Pseudonymisierung, Konzepte zur Datenminimierung, zum Datenzugriff, zur Datenlöschung (Art 25).
☑	**Datenrichtigkeit und Datenaktualität:** Personenbezogene Daten müssen sachlich richtig und auf dem neuesten Stand sein. Personenbezogene Daten, die im Hinblick auf ihre Zwecke unzutreffend sind, sind unverzüglich zu löschen oder zu berichtigen. Regelungen zu Korrekturprozessen, sobald Datenunrichtigkeiten bekannt werden, sind festzulegen (Art 5 Abs 1 lit d).
☑	**Beschränkung der Speicherdauer:** Daten dürfen nur so lange gespeichert werden, wie dies zur Erreichung der mit der Datenverarbeitung verfolgten Zwecke erforderlich ist. Die Speicherdauer bzw. die Kriterien zur Festlegung der Speicherdauer sind anzuführen (Art 5 Abs 1 lit e).
☑	**Einhaltung der Anforderungen an Datensicherheit:** Personenbezogene Daten sind so zu verarbeiten, dass sie vor unbefugter oder unrechtmäßiger Verarbeitung, vor zufälligem Verlust, zufälliger Zerstörung oder Schädigung geschützt sind. Dazu sind geeignete technische und organisatorische Maßnahmen zu treffen (Art 5 Abs 1 lit f).
☑	**Datenübermittlung an Dritte:** Hinweis auf Empfänger von Daten oder Kategorien von Datenempfängern und Hinweis auf Übereinstimmung mit dem berechtigten Zweck; bei Datenübermittlung an Drittländer darf das Schutzniveau für die Betroffenen (geeignete Garantien, durchsetzbare Rechte und wirksame Rechtsbehelfe) nicht

[1] Die folgende Checkliste entstammt dem Buchbeitrag *Angerler/Reven*, DSGVO und nationales Arbeitsrecht, in Knyrim (Hrsg), Datenschutz-Grundverordnung. Das neue Datenschutzrecht in Österreich und der EU (2016).

	untergraben werden. Es ist ein Hinweis auf Maßnahmen zur Sicherung eines angemessenen Datenschutzniveaus erforderlich (Art 44–50).
☑	**Aufklärungs- und Informationspflichten:** Klare und leicht verständliche Informationen zur Datenverarbeitung müssen vorhanden sein, sowie Modalitäten für die effektive Ausübung der Rechte der betroffenen Person. Über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling muss ausdrücklich informiert werden, in diesem Fall sind den Betroffenen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung zu übermitteln (Art 12–14).
☑	**Hinweis auf Betroffenenrechte** (Art 15–20) und deren Ausübung, und zwar das Recht auf Auskunft, auf Berichtigung, auf Löschung von Daten zur eigenen Person sowie das Recht auf Widerspruch, insb. bei Profiling (Art 21–22).
☑	**Sicherstellung rechtmäßiger Auftragsdatenverarbeitung:** Vorhandensein von Garantien, die die Eignung des Auftragsverarbeiters sicherstellen, verordnungskonforme Datenverarbeitungen durchzuführen; Vorhandensein eines (Dienstleister-)Vertrages, der Art, Zweck und Dauer der Verarbeitung sowie Art der personenbezogenen Daten und Kategorien der betroffenen Personen enthält; Berücksichtigung der Betriebsvereinbarung durch den Auftragsdatenverarbeiter (Art 28).
☑	**Ergebnis der Datenschutz-Folgenabschätzung und der Risikoeinschätzung** – wenn erforderlich – prüfen (Sicherheitskonzept), insb bei automatisierten Einzelentscheidungen und Profiling sowie bei Verwendung besonderer Datenkategorien (Art 35).
☑	**Vorab-Konsultationspflicht** bei risikoreichen Datenverarbeitungen – schriftliche Empfehlungen der Aufsichtsbehörde umsetzen (Art 36).

DATENSCHUTZPRAXIS FÜR BETRIEBSRÄTE
QUICKCHECK: WO STEHEN WIR HEUTE?

Dieser Fragenbogen dient der raschen Selbsteinschätzung der eigenen (betriebsrätlichen) Situation im Bezug auf Datenschutzfragen.

Es geht hier nicht um Bewertung oder Beurteilung sondern nur darum, Aufmerksamkeit auf dieses wichtige Thema zu lenken.

GENERELLE FRAGEN

- Gibt es eine betriebliche Organisation (Rollen, Prozesse, Kultur) für Datenschutzfragen?
- Gibt es einen betrieblichen Datenschutzbeauftragten (im Betrieb, im Konzern, Inland oder Ausland)?
- Wer vermittelt zwischen DS Fragen und arbeitsrechtlichen Anfragen des BR? (also zwischen EUDSGVO und ArbVG & Co)
- Wieviele betriebsinterne Anwendungen kennst du in deinem Betrieb?
- Gibt es einen kommunizierten Prozess zur Genehmigung interner Anwendungen?
- Welche Arten von Anwendungen gib es in deinem Betrieb?
    - Standardanwendungen (zB Personalwesen, Gehaltsverrechnung, …)
    - Security Tools (Interne Kontrollanwendungen zur Netzsicherheit mit oft weitreichenden Möglichkeiten)
    - Big Data Datenbank, die als Basis für analytische Software oder kognitive AI Anwendungen verwendet werden können
    - Gibt es Diskussionen zu Big Data, Algorithmen, Ethik & Werten?
- Sind die Bedingungen zur Anwendung betriebsintern verwendeter Software klar geregelt?
    - Gibt es eine Rahmen BV zum Datenschutz
    - Gibt es weitere Betriebsvereinbarungen?

- Gibt es dokumentierte „Betriebsbedingungen“

DER BETRIEBSRAT ALS BERATER

- Sind die Unternehmensspielregeln im Bezug auf Arbeitsmittel, Hardware, Software klar geregelt und kommuniziert?
- Wurden die Mitarbeiter in eurem Betrieb von der GL ausreichend über Datenschutz informiert?
- Informieren euch MitarbeiterInnen über Probleme mit betriebsinterner Software?
- Wer ist euer betrieblicher Ansprechpartner bei derartigen Problemmeldungen?

DER BETRIEBSRAT ALS KONTROLLOR

- Welche Rechte nehmt ihr derzeit im Bezug auf Datenschutz tatsächlich wahr? (Beratung, Kontrolle, Intervention)
- Habt ihr Listen, wann ihr welche Kontrollen im Bezug auf betriebsinterne Anwendungen durchführt?
- Bekommt ihr Aufmerksamkeit bzw. vernünftige Antworten auf eure Datenschutzanfragen und Problemmeldungen?

DER BETRIEBSRAT ALS VERANTWORTLICHER isd EU-DSGVO

- Arbeitet der BR DSGVO konform (zumindest seit 25.5.2018)?
    - Verwendet ihr die AK/Forba Templates?
    - Habt ihr ein Verarbeitungsverzeichnis?
    - Habt ihr die MitarbeiterInnen über die von euch verarbeiteten Daten informiert?
    - Gibt es in eurem BR Gremium gute Techniker?
    - Gibt es in eurem BR Gremium juristische Kenntnisse?