**30.5.2018**

**Datenschutz-Management im Betriebsrat – betriebliche Erfahrungen bei IBM / Tom Gödel, BRV bei IBM**

Empfehlenswert:

Film Democracy – im Rausch der Daten (Dauer 1,5h)

Film: Citizen Four (Dokumentation über Edward Snowden, erst durch sein Outing ist vielen in dieser Zeit klar geworden, dass Regelungsbedarf besteht)

Vorgehen bei IBM, Ansatz nach Thomas Riesenecker-Caba:

* Awareness im Betriebsratsteam, Europäischen Betriebsrat (IBM ist in 18 EU-Ländern vertreten)
* Thema im Aufsichtsrat (Compliance)
* Awareness/Transparenz bei der Belegschaft, bei Betriebsversammlungen: welche Tools gibt es, welche Daten werden verarbeitet, Aufmerksamkeit bei Mitarbeitern schaffen (oft wird auf Mitarbeiter zugegangen, dass sie schnell eine Liste aus einem System ziehen sollen – Frage der Zulässigkeit)

Einführung von neuen Systemen:

* Einerseits die Mitbestimmungsrechte aufgrund des Arbeitsverfassungsgesetzes wahrnehmen, andererseits Einfordern des Datenschutz aufgrund der Kontrollfunktion des Betriebsrats
* Größte Schwierigkeit im Verstehen der Systeme, es ist von großem Vorteil, wenn man im Betriebsratsteam einen Techniker und Juristen hat. Falls dies nicht der Fall ist, abklären welche Grundlage ist im BR-Gremium im Bezug auf Datenschutz vorhanden, was kann zukünftig abgedeckt werden, wichtig Netzwerken zu anderen Betriebsräten, Fachgewerkschaften.
* Betriebsrat soll auf Basis der ArbVG bei Einführung von System auch den Datenschutz und die Verantwortung einfordern (Risiko).
* Beim IBM-BR gibt es einen gewissen Automatismus, um rasch weitere Vorgangsweise entscheiden zu können, z.B. gibt es bereits ein ähnliches System, eine Betriebsvereinbarung, ist es etwas komplett Neues, etc. Bei IBM gibt es ca. 50 BVs, davon ca. 15 für den Datenschutz.

Schulungen:

* Bei IBM müssen weltweit ALLE Mitarbeiter eine Schulung zur europäischen DSGVO absolvieren, alle müssen die Risiken, Haftungen verstehen, wenn sie Daten für Österreich/Europa verarbeiten.
* Bei IBM wird für alle Mitarbeiter ein generisches Schulungsprogramm durchgeführt, Details gibt es dann in jeweiligen Businessbereichen.
* Empfehlung: Als Betriebsrat nachzufragen: welche Schulungen es für die Mitarbeiter zur DSGVO gibt / wie ist der Umgang mit den ArbeitnehmerInnendaten

Verantwortung:

* Erfahrungen aus anderen Betrieben: es wurden Datenschutz-Koordinatoren eingesetzt, Haftung wird suggeriert, Verantwortlichkeit wird möglichst weit runter delegiert.

BR als Veranwortlicher:

* Erster Schritt: Klärung „was tun wir eigentlich?“

|  |  |
| --- | --- |
| **Ziele****Mission****Credo****Vorbild** | **Betriebsrat****Blue Print** |
| **Operation = tägliches Geschäft:**Beratungen, BR-Fonds, Kassaführung, BR-Büro, Dienstleistungen (z.B. Versicherungen), Benefits | **Projekte:**Betriebsversammlungen, Fokustage, Ausflug, Wahl (BR, AK, Jugendvertrauensrat), Lachsverkauf, Weih. Feier, Gutscheinaktion, Töchtertag, Apothekenlieferung |
| **Rollen:**BRV, BRV-Stellvertr., Schriftführer, Kassier, Aufsichtsrat, Data Privacy Officer, Beirat für Pensionskasse, EBR, KBR | **Netzwerken**Fachgewerkschaften, AK, betriebsfremde Betriebsräte |
| **Themen:** Wirtschaft (bei Wirtschaftsgesprächen, Aufsichtsrat), Datenschutz, Gehalt, Arbeitszeit, Sicherheit, BR-Wahl, etc. |
| **§§: Gesetze, KV, Betriebsvereinbarungen, Judikatur** |

* Für jedes einzelne Thema anschauen, z.B. Arbeitszeit, welche Daten haben wir (elektronisch, Papier), welche bekommen wir von HR. Empfehlung um auch in Zukunft sicherzustellen, dass BR gewisse Reports erhält, mit HR besprechen, welche Reports derzeit zur Verfügung gestellt werden.
* Setup im BR-Team festgelegt, Vereinbarung dieses einzuhalten: Beschluss
* Ausnahme: wenn ein BR-Mitglied selber Daten verarbeitet (z.B. bekommt von einem Mitarbeiter Daten und verarbeitet diese z.B. auf seinem privaten PC) dann ist dieses Mitglied selber „Verantwortlicher“: Beschluss

Offenes / größte Challenge ist die Löschung:

* Datenschutz ist ein Entwicklungsprozess, Offenes in einer Aktionsliste mit Verantwortungen, to do’s, Deadlines festhalten. 2 x jährliche Inventur. Dann kann man der Datenschutzbehörde vorweisen, dass man bei diesen Themen bereits dran ist.
* Risikominimierung, wenn z.B. Löschregelungen noch nicht klar, Einschränkungen bei den Zugriffen, Sicherheit, etc.

Transparenz / Information an die Mitarbeiter:

* Aussendung an Mitarbeiter, BR sieht sich als Verantwortlicher, Info welche Daten der BR aufgrund Gesetze, etc. verarbeitet, im Intranet veröffentlicht
* **Kommunikation: Template von Eva Angerler**

Personenbezogene Daten / Beispiele:

* Apothekenlieferung: Mitarbeiter schickt seine Bestellung per E-Mail direkt an Apotheke (andere Betriebe haben auch Onlinebestellungen direkt bei der Apotheke) / Lieferung mit Medikamenten an Betriebsrat, Verteilung durch Betriebsrat (Medikamente +Rechnung im Sackerl) (bei anderen Betrieben wird Rechnung direkt an die Privatadresse des Mitarbeiters geschickt.
Betriebsrat hat hier zumindest Vermittlertätigkeit, deshalb ist BR Verantwortlicher.
Achtung auf Datenminimierung!
* Beratung: bei der persönlichen Beratung Mitschrift am Block, wird danach in den PC übertragen, Zugriff 3 BR (BRV, BRV-Stellvertr., Schriftführer).

Technische & organisatorische Maßnahmen:

* Schlüssel im BR-Büro?
* Bei IBM hat jeder Mitarbeiter (und somit auch der BR) jährlich Dokumente zu unterschreiben, dass Geschäftsprozesse eingehalten werden, Passwörter vergeben werden, etc., diese unterschriebenen Dokumente sind dann auch für den BR als Vorlage bei der Datenschutzbehörde, dass sich BR compliant verhält