# Informationsblatt zur Erstellung eines Informations-sicherheits- und Datenschutz-Managementsystems (INFO 4)

Bei der Verarbeitung von personenbezogenen Daten sind auch die Anforderungen zur Daten- und IT-Sicherheit zu prüfen und zu dokumentieren (im Betrieb können die betrieblich vereinbarten Maßnahmen auch in anderslautenden Dokumenten wie zB *IT-Policy* oder *IT-Sicherheitsleitlinien* veröffentlicht sein).

Wir empfehlen die in der Checkliste "*Prüfung der organisatorischen, personellen und technischen Sicherheitsmaßnahmen zur IT-Sicherheit (CHECK 2)*“ angeführten Prüfschritte durchzuführen und daraus abgeleitete Maßnahmen und Regeln für die BR-Körperschaft zu beschreiben.

Die in Folge angeführten Textbausteine dienen dabei zur Orientierung und können für die Dokumentation der eigenen Maßnahme zur IT-Sicherheit (DOKU 3) nach Prüfung im Betriebsrat verwendet werden.

Folgende Vorschläge zur IT-Sicherheit können für die Betriebsratsarbeit und die Arbeit im Betriebsratsbüro - zusätzlich zu den betrieblichen Anforderungen (sofern vorhanden) - vom BR-Zuständigen für Datenschutz erlassen werden.

**Organisatorische Sicherheitsmaßnahmen**

* Personenbezogene Daten und vertrauliche Dokumente (von Arbeitnehmer/innen, vom Arbeitgeber, von Dritten) dürfen nicht auf privaten Geräten gespeichert werden, außer es wurde ausdrücklich gestattet und es sind zusätzliche Sicherheitsmaßnahmen zum Schutz dieser Daten und Dokumente vereinbart worden.
* Neue Software und neue Apps, die vom BR installiert wird, sind auf Geräten, auf denen sich personenbezogene Daten von Mitarbeiter/innen befinden, nur nach Prüfung zu verwenden. Die Geschäfts-/Nutz­ungsbedingungen sind im Hinblick auf die Anforderungen der DS-GVO/des DSG zu prüfen und abzulegen.
* Das Speichern von personenbezogenen Daten und/oder Dokumenten bei externen Cloudanbietern ist nur nach Prüfung der datenschutzrechtlichen Anforderungen gestattet.
* Daten/Dokumente von Mitarbeiter/innen oder Informationen aus dem Betriebsrat, die sich auf privaten Geräten des Betriebsrates befinden, sind regelmäßig zu sichern, damit diese nicht verloren gehen können. Nicht mehr notwendige Daten/Dokumente sind zu löschen.
* Daten/Dokumente werden in folgende Sicherheitsklassen unterteilt:

a) *öffentliche Daten/Dokumente*: diese können ohne Einschränkung betrieblich verwendet und veröffentlicht werden

b) *interne Daten/Dokumente*: diese stehen nur innerhalb des Betriebsrates zur Verfügung und dürfen nur nach Prüfung an berechtigte Dritte weitergegeben werden

c) *vertrauliche Daten/Dokumente*: diese dürfen nur von ausgewählten Mitgliedern des Betriebsrates verwendet werden

d) *geheime Daten/Dokumente*: diese stehen ausschließlich vorab definierten Personen zur Verfügung und sind betrieblich besonders zu schützen

* Die Betroffenenrechte (z.B. gegenüber Mitarbeiter/innen) sind im Sinne der rechtlichen Anforderungen zu erfüllen. Die betroffenen Personen werden darüber und über ihre Rechte gemäß Datenschutzrecht (z.B. auch in Formularen) informiert.
* Die im Betriebsrat vereinbarten und getroffenen Maßnahmen werden dokumentiert (siehe DOKU 3) und regelmäßig auf ihre Anwendbarkeit geprüft (Evaluierung).

**Personelle Sicherheitsmaßnahmen**

* Für dienstliche Geräte (vom Arbeitgeber zur Verfügung gestellt) wie PC, Laptop, Smartphone, Datenträger (z.B. USB) sind die im Betrieb definierten Regelungen - z.B. bzgl. Passwortgestaltung, Virenschutz oder Datensicherung einzuhalten.
* Geräte für die Betriebsratsarbeit sind zu schützen (z.B. Passwort, Ausloggen bei Verlassen des Arbeitsplatzes) und Zugangsdaten zu diesen Geräten dürfen nicht an Dritte weitergegeben werden.
* Die datenschutzrechtliche Aufgabenverteilung und Zuständigkeiten im Betriebsrat und im BR-Büro sind ausdrücklich festzuschreiben und zu dokumentieren.
* Betriebsräte unterliegen nach ArbVG einer gesetzlichen Verschwiegenheit, daher ist vor Weitergabe von Daten zu prüfen, ob dies im Sinne der gesetzlichen Bestimmungen auch zulässig ist. Ersatzmitglieder dürfen nur diejenigen Daten/Dokumente erhalten, wenn sie diese im Rahmen ihrer konkreten Vertretungstätigkeit benötigen.
* Mitarbeiter/innen im BR-Büro, die keine Tätigkeit als Betriebsrat ausüben, sind - zusätzlich zur betrieblichen Verschwiegenheit - gesondert zur Geheimhaltung der im Arbeitsalltag bekannt gewordenen Informationen zu verpflichten.
* Bei Ausscheiden aus dem Betriebsrat sind alle relevanten Daten und Dokumente, die während der BR-Tätigkeit entstanden bzw. bekannt geworden sind, sofern diese noch benötigt werden nach Rücksprache mit dem/der BR-Vorsitzende/r und dem/der Zuständigen für Datenschutz im BR zurückzugeben und erst dann zu löschen.
* Beim Ausscheiden aus dem Betriebsrat bzw. dem BR-Büro (bei Admin-Beschäftigten) sind die dienstlichen Betriebsmittel (PC, Laptop, Smartphone aber auch Schlüssel/Zutrittskarten) zurückzugeben. Gegebenenfalls sind auf den Endgeräten befindliche Daten vor bzw. nach Übergabe an den/die BR-Vorsitzende/n bzw. die für Datenschutz im BR zuständige Person zu löschen.
* Der Zuständige für Datenschutz im Betriebsrat weist regelmäßig (2-3/Jahr) im Rahmen von BR-Sitzungen auf die Anforderungen zu Datenschutz und Datensicherheit und die vereinbarten Sicherheitsleitlinien (Spielregeln) hin.
* Bei Verlassen des Arbeitsplatzes und/oder des Büros ist der Systemzugang zu sperren und Papierdokumente vor dem Einblick Unberechtigter zu schützen bzw. zu versperren.
* Betriebsratsmitglieder und Mitarbeiter/innen im BR-Büro sind zum Datenschutz und den getroffenen Regelungen der Verarbeitung personenbezogener Daten zu schulen.

**Technische Sicherheitsmaßnahmen (je Verarbeitungstätigkeit zu prüfen!)**

* Bei Geräten (PC, Laptop, Smartphone, Datenträger) und Programmen/Apps bzw. im Ablagesystemen (elektronisch und Handakte) ist zu prüfen, wer darauf Zugriff benötigt und die notwendigen Rechte sind zu vergeben und regelmäßig zu prüfen.
* Auf privaten Geräten, auf denen sich personenbezogene Daten/Dokumente befinden, sind die Zugriffsberechtigungen sowie die Betriebssoftware und der Virenschutz aktuell zu halten, Passwörter sind sicher zu gestalten und zu ändern, wenn die Gefahr besteht, dass Dritte davon Kenntnis erlangt haben.
* In öffentlichen WLANs (die oft nicht ausreichend gesichert sind) ist besondere Vorsicht im Umgang mit personenbezogenen Daten walten zu lassen, bei Arbeiten oder Telefonieren im öffentlichen Raum sind die betrieblichen Daten zu schützen.
* Bei Datenübermittlung (E-Mail, Messenger wie WhatsApp oder soziale Medien wie Facebook) sind vertrauliche Daten, wenn technisch möglich, zu schützen (Verschlüsselung, zip-Dateien mit Passwortschutz, Dokument mit Kennwortschutz).
* Daten auf mobilen Datenträgern (z.B. USB) können leicht verloren gehen und sind daher besonders zu schützen.
* Beim Öffnen von Mailanhängen bzw. dem Anklicken eines Links in Mails oder im Internet ist darauf zu achten, dass keine Gefahr für die betriebliche Infrastruktur entstehen kann.
* Als besonders schutzwürdig eingestufte Datenverarbeitungen sind zu protokollieren, auch hinsichtlich der Person des auf die Daten Zugreifenden (etwa durch die Software oder händisch zu dokumentieren).
* Die Verwaltung von Schlüsseln/Zutrittskarten zum BR-Büro und zu versperrbaren Kästen mit Dokumenten ist zu dokumentieren.
* BR-Dokumente und Daten sind gesichert zu speichern und nach Zweckerreichung zu löschen bzw. zu vernichten.