ifb
Seminare,
die begeistern

Datenschutz im Betriebsrat

ifb-Ratgeber

Wissenswertes rund um den Datenschutz

www.ifb.de/datenschutz

Liebe Nutzer von mein ifb,

„Hacker-Angriff auf die Bundesregierung“, „Snowden enthüllt: NSA-Überwachung in Deutschland“, „Lidl muss Millionenstrafe wegen geheimer Krankenakten zahlen“ – diese Schlagzeilen der vergangenen Jahre verunsichern uns. Wie geht der Arbeitgeber mit meinen Daten um? Wie kann ich mich vor Angriffen auf sensible Daten schützen – im Betriebsrat und privat?

Mit diesem Ratgeber möchten wir die dringlichsten Fragen rund um das Thema Datenschutz für Sie erläutern. Außerdem finden Sie hier grundlegende Informationen zur EU-Datenschutzgrundverordnung, die im Mai 2018 in Kraft tritt. Für die Datenschutzbeauftragten Ihres Unternehmens ändert sich damit einiges – doch auch Sie als Betriebsrat sollten die wichtigsten Grundlagen dieser Verordnung kennen.

Wir wünschen Ihnen viel Spaß beim Lesen und viel Erfolg in Ihrem Amt!

Ihre ifb-Redaktion

INHALT

Was ändert sich für mich als Betriebsrat durch die Datenschutz-grundverordnung?

Mit der EU-Datenschutzgrundverordnung (EU-DSGVO) werden die Standards für den Datenschutz innerhalb der EU auf ein gemeinsames Niveau angehoben. Die Umsetzung der DSGVO erfolgt in Deutschland durch ein novelliertes Bundesdatenschutzgesetz. Ein Schritt, der lange überfällig war – denn weite Teile unseres Datenschutzgesetzes stammten bisher noch aus dem Jahr 1990, als Unternehmen sich noch nicht mit elektronischen Bewerbungsverfahren, Zeiterfassungssoftware und Internetnutzung beschäftigen mussten.

Für Betriebsräte werden dann insbesondere die Auswirkungen der neuen Gesetzeslage auf bestehende und neue Betriebsvereinbarungen relevant. Bisher war die Verarbeitung von personenbezogenen Daten nur dann zulässig, wenn es das BDSG oder eine andere Rechtsvorschrift erlaubt oder aber der Betroffene selbst eingewilligt hat. Solche andere Rechtsvorschriften konnten beispielsweise Betriebs- und Dienstvereinbarungen sein.

Ab 25. Mai 2018 gelten deutschland- und europaweit neue Datenschutzgesetze.

Ein wichtiges Thema für jeden Betriebsrat!

Im neuen Datenschutzgesetz werden solche Vereinbarungen nun unter dem allgemeinen Titel „Kollektivvereinbarungen“ genannt. Diese können sowohl Tarifverträge, als auch Betriebsvereinbarungen sein. Sie stehen im Gesetz gleichberechtigt nebeneinander – in Art. 88 Abs. 1 EU-DSGVO sind jedoch inhaltliche Kriterien unter anderem für Kollektivvereinbarungen festgelegt. Sie umfassen beispielsweise die Gesundheit und Sicherheit am Arbeitsplatz, Einstellung und Beendigung des Beschäftigtenverhältnisses, aber auch die für die Betriebsparteien besonders relevante „Inanspruchnahme kollektiver Rechte und Leistungen“. Außerdem sind Arbeitgeber verpflichtet, berechtigte Interessen und Grundrechte der betroffenen Personen zu berücksichtigen. Viele dieser Grundsätze mussten bereits nach dem alten Gesetz bei dem Abschluss von Betriebsvereinbarungen beachtet werden. Jetzt finden sich diese auch im Gesetz verankert wieder.

Beim Verfassen einer neuen Betriebsvereinbarung muss nun berücksichtigt werden, dass das Datenschutzniveau der DSGVO nicht unterschritten werden darf. Neu ist dabei die Transparenz bei der Verarbeitung personenbezogener Daten – sie muss nach Art. 88 Abs. 2 EU-DSGVO gesondert berücksichtigt werden.

Dieser Punkt muss auch in bestehenden Betriebsvereinbarungen angepasst werden. Bisher war es nicht verpflichtend, auf die Rechte der betroffenen Arbeitnehmer in einer Betriebsvereinbarung einzugehen. Die DSGVO macht diesen Schritt nun unumgänglich.

Praxis-Tipps:

Wenn Sie im Betriebsrat eine neue Betriebsvereinbarung verfassen möchten, sollten Sie insbesondere folgende Punkte deutlich regeln bzw. berücksichtigen:

- Die Informationspflicht der betroffenen Personen bei der Erhebung von Daten
- Die Auskunftsrechte der betroffenen Personen
- Das Recht auf Berichtigung, Löschung („Das Recht auf Vergessenwerden“) und Sperrung der eigenen Daten und die damit verbundenen Mitteilungspflichten
- Das Recht auf Datenübertragbarkeit
- Das Widerspruchsrecht
- Die Rechte bei Profiling-Maßnahmen

Seminar-Tipps:

Gremiumsmitgliedern, die sich bereits im Datenschutz etwas auskennen und die nun eine IT-Betriebsvereinbarung verfassen bzw. mit dem Datenschutz im Unternehmen betraut sind, empfehlen wir das Seminar **„Datenschutzrecht 2018: Doppelter Handlungsbedarf für den BR“**. Hier lernen Sie alle wichtigen Änderungen durch die beiden neuen Gesetze kennen: von den neu zu beachtenden Pflichten bis hin zu den Folgen für alte oder neue Betriebsvereinbarungen. Spannende Herausforderungen für Betriebsräte, aber auch willkommener Anlass, den Datenschutz im Betrieb zu überprüfen!

› www.ifb.de/23

Für Gremiumsmitglieder ohne Datenschutzvorwissen empfehlen wir das Seminar **„Der Gläserne Mitarbeiter I“**. Der ideale Einstieg ins Thema Datenschutz: Hier erhalten Sie alle wichtigen Grundlagen, um auch in Zukunft den Datenschutz in Ihrem Betrieb rechtssicher zu gestalten.

› www.ifb.de/68

Was ist ein sicheres Passwort?

Dass „passwort“ oder „123456“ keine sicheren Passwörter sind, wissen heutzutage die meisten Nutzer. Doch mit einem sogenannten „Wörterbuchangriff“ lassen sich die meisten Passwörter innerhalb weniger Minuten knacken. Ein Wörterbuchangriff ist ein Programm, das die häufigsten Passwörter automatisch austestet und so meistens einen Treffer landet. Denn: Unser aktiver Wortschatz liegt durchschnittlich bei 50.000 Wörtern. Supercomputer sind in der Lage, bis zu 33 Billiarden Passwörter pro Sekunde zu testen. Kombiniert der Wörterbuchangriff also Begriffe, häufige Namen und Zahlen (insbesondere Geburtsdaten) miteinander, ist das Passwort meistens schnell gefunden – und Ihre Daten sind nicht mehr geschützt. Schlimmer noch: Wenn ein Hacker erst einmal Zugang zu Ihrem privaten E-Mail-Account, Ihrem Bankkonto oder anderen sensiblen Daten hat, stehen ihm Tür und Tor für weitere Betrugsdelikte offen.

Ein sicheres Passwort sollte darum nie nur aus einem („Passwort“) oder zwei („MeinPasswort“) Wörtern bestehen. Es sollte außerdem mindestens acht, besser noch zwölf Zeichen enthalten.

Praxis-Tipps:

UM EIN SICHERES PASSWORT ZU ERSTELLEN, EMPFEHLEN WIR IHNEN ZWEI WEGE:

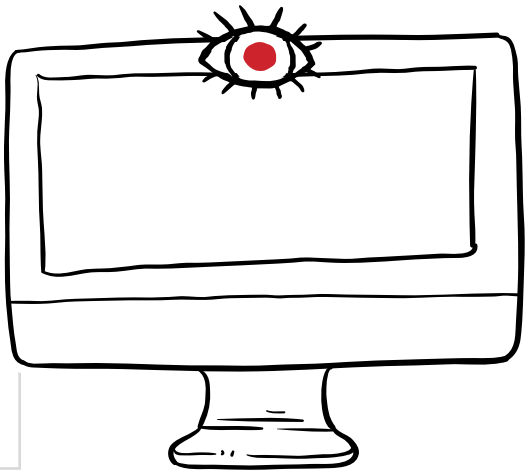
1. Nutzen Sie einen Passwort-Generator. Auf Seiten wie **www.sicherespasswort.com** können Sie schnell und kostenlos sichere Passwörter generieren. Diese bestehen aus zufälligen Kombinationen aus Buchstaben, Zahlen und Sonderzeichen wie beispielsweise %, & oder !
Es ist natürlich nicht ganz einfach, sich so eine zufällige Reihenfolge zu merken. Notieren Sie sich Ihre Passwörter daher am besten ganz altmodisch handschriftlich – in einem Notizbuch oder an einem anderen Ort, der für Dritte unzugänglich ist.

2. Bilden Sie sich Ihre persönliche Eselsbrücke. Aussagen, die wir mit einem Gefühl verbinden, können wir uns dabei besonders gut merken. Haben Sie eine schöne Erinnerung an einen vergangenen Urlaub? Dann bilden Sie daraus einen Satz, beispielsweise „Picknick im Urlaub im Juni mit Susi am Lago Maggiore“.
Kürzen Sie diesen nun in Form eines Passworts ab:
PNiUi06+S@LM

Weitere Tipps zum Schutz Ihrer Daten

Facebook-Gründer Mark Zuckerberg tut es, der ehemalige FBI-Chef James Comey tut es auch: Sie kleben die Kamera ihres Laptops bzw. Smartphones ab. Comey begründete diesen Schritt folgendermaßen:

„Ich habe gesehen, dass eine Person, die schlauer ist als ich, die Kamera abgeklebt hat."



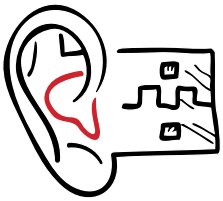
Praxis-Tipp:

Kleben Sie Ihre Kamera am Smartphone bzw. am Laptop mit einem Stück Papier oder ähnlichem ab. Für Smartphones gibt es auch spezielle Plastikdeckel, die sie für gelegentliche Schnappschüsse schnell und unkompliziert entfernen können.

Es gibt mehrere Gründe, weshalb Sie sich sich vor ungewollter Beobachtung schützen sollten:

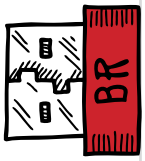
Zum Einen schenken Nutzer Ihrer Webcam meist wenig Beachtung. In einer Untersuchung der University of California, Berkeley, konnte gezeigt werden, dass ein Großteil der Testpersonen es nicht bemerkte, als die zur Kamera gehörende LED-Lampe gelegentlich an und wieder aus ging. Zum anderen lässt sich dieses Lämpchen leicht manipulieren. Hacker finden die nötige Software zum Abschalten der LED-Lampe im Netz – sie müssen also noch nicht einmal selbst brillante Programmierer oder professionelle Internet-Betrüger sein. Besonders anfällig für so einen Angriff sind Apple-Geräte.

Eine Studie des Digitalverbandes Bitkom ergab, dass mittlerweile bereits jeder vierte Nutzer seine Kamera abklebt. IT-Sicherheitsexperten empfehlen, zusätzlich noch das Mikrofon am Laptop abzukleben – zumindest, wenn sich das Gerät in einem Raum befindet, in dem vertrauliche Gespräche geführt werden, wie beispielsweise im Betriebsratsbüro. Der Einfachheit halber können Sie auch eine Keksdose (aus Metall) im Betriebsratsbüro aufbewahren. Zu Beginn der Sitzung legen alle Anwesenden Ihr Smartphone in diese Dose - so hat Ihr Telefon weder Empfang, noch kann das Mikrofon etwas aufzeichnen.



Doch auch ohne Schadsoftware ist ein Lauschangriff möglich: Die aus Spionagefilmen bekannten Wanzen sind heute oft als unauffälliger USB-Stick getarnt. Sie müssen zur Aufnahme nicht an einen Laptop angeschlossen sein, sondern können unauffällig in Hörweite deponiert werden und erst dann mit der Aufnahme beginnen, wenn Geräusche in der näheren Umgebung erzeugt werden. Sogenannte „Wanzenfindergeräte" gibt es zwar schon für kleines Geld – sie sind aber nur dann sinnvoll und einsatzbereit, wenn sich keine weiteren Elektrogeräte im Raum befinden. Somit scheiden sie für die meisten Betriebsratsbüros aus.

Falls Ihr Gremium abgehört wurde, erstatten Sie unverzüglich Anzeige. Das heimliche Abhören Dritter – egal, ob es am Arbeitsplatz oder im Privatleben stattfindet – ist ein Vergehen nach § 201 Abs. 1 und 2 StGB („Verletzung der Vertraulichkeit des Wortes“) und wird mit Freiheitsstrafe bis zu drei Jahren oder einer Geldstrafe bestraft.



Praxis-Tipp:

Legen Sie im Gremium fest, welche USB-Sticks von Ihnen verwendet werden. Halten Sie Ordnung im Betriebsratsbüro, sodass ein „fremder“ USB-Stick schneller auffällt. Sollte Sie dennoch einen unbekannten USB-Stick finden, prüfen Sie, ob sich darauf Audio-Dateien (.mp3, .wav, .m4a oder .flac-Format) befinden und überprüfen Sie diese gegebenenfalls.

Ein weiterer Weg zur Ausspähung Ihrer Daten sind sogenannte Keylogger. Diese zeichnen auf, was über die Tastatur Ihres Computers eingegeben wird. Dabei werden zwei Arten von Keyloggern unterschieden: Software- und Hardware-Keylogger.

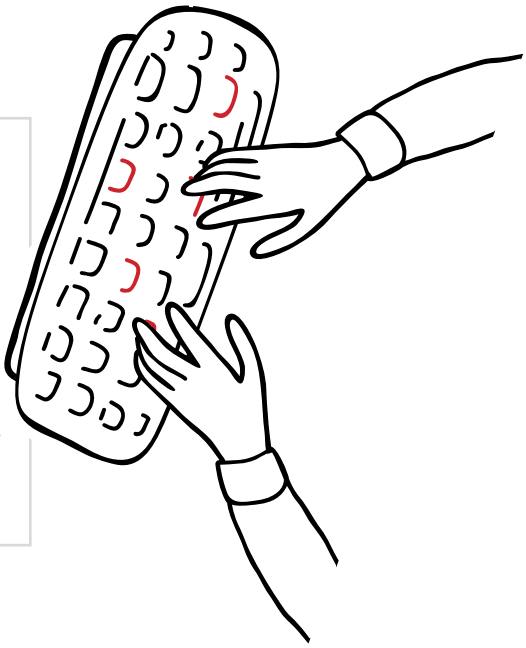
Software-Keylogger sind Programme, die die Tastendrucke direkt an das Betriebssystem weitergeben. Sie können die Daten lokal auf einer Festplatte speichern oder direkt an einen weiteren Rechner senden.

Hardware-Keylogger sind direkt zwischen die Tastatur und Rechner gesteckt – sie können in Form eines USB-Sticks oder Zwischensteckers zur Tastatur auftreten. Die ausgespähten Daten werden auf dem Keylogger gespeichert und können nach der Entfernung ausgelesen werden. Der Einsatz von Keyloggern ohne das Einverständnis des Nutzers ist gemäß § 202a StGB strafbar. Möchten Unternehmen Keyloggern an ihren Firmencomputern einsetzen, müssen sie zuvor die Zustimmung des Betriebsrats einholen. Doch auch in Unternehmen ohne Betriebsrat dürfen Keylogger nicht ohne das Wissen der Nutzer verwendet werden: Der Arbeitgeber muss die Belegschaft informieren.

Gut zu wissen:

Software-Keylogger werden mit Anti-Spyware-Programmen oder Virenscannern gefunden. Aktualisieren Sie Ihren Virenscanner daher regelmäßig. Hardware-Keylogger können Sie durch eine Überprüfung der Tastatur bzw. Ihres Rechners entdecken.

Um ganz sicher zu gehen, können Sie auch eine sogenannte virtuelle Tastatur nutzen. Diese funktioniert wie eine Tastatur am Smartphone – die meisten PCs verfügen über eine virtuelle Tastatur, die in einem eigenen Anwendungsfenster geöffnet wird.



ifb
Seminare,
die begeistern

Herausgeber:
ifb Institut zur Fortbildung
von Betriebsräten KG
Prof.-Becker-Weg 16
82418 Seehausen am Staffelsee

Tel.: 0 88 41 / 61 12-0
Fax: 0 88 41 / 61 12-151
E-Mail: info@ifb.de

Internet:
www.ifb.de
www.betriebsrat.de
www.facebook.com/ifbKG
www.twitter.com/ifbKG

Geschäftszeiten:
Mo - Do: 8:00 - 17:00 Uhr
Fr: 8:00 - 16:00 Uhr

Verantwortlich:
Hans Schneider

Redaktion:
Jessica Riccò
Stephan Sägmüller
Claudia Lohmar

Fotos:
BlackJack3D_iStock (1),
Kristina Kömpel-Schütz (8)

Hinweis:
Die verwendete maskuline bzw. feminine Sprachform dient der leichteren Lesbarkeit und meint immer auch das jeweils andere Geschlecht.

Stand: März 2018

Unsere Mitarbeiter sind für Sie da – bei Fragen zu unserer Website, Ihrer Seminarreservierung bzw. unserem Seminarangebot. Oder wenn Sie Informationen über Ihr Hotel benötigen, Ihren Schulungsanspruch klären möchten oder Näheres über den Ablauf des Seminars wissen möchten. Wir freuen uns über Ihren Anruf!

IHR INFO- & SERVICETEAM

Sieglinde Gailer, Barbara Neuner, Karina Bergfeld, Anna Sophie Halemba, Christine Dietrich, Barbara Ketzer, Monika Fruth, Dominica Gilg, Silvia Hebendanz, Marcella Panuccio

Sie erreichen uns von Montag bis Donnerstag

8:00 Uhr – 17:00 Uhr und am Freitag 8:00 – 16:00 Uhr.

› Tel. 0 88 41 / 61 12-0

› E-Mail: info@ifb.de

Neu im Betriebsrat?
Dann gleich bei „mein ifb“ anmelden und Vorteile nutzen
› www.mein-ifb.de

www.ifb.de