Leitfaden Datenschutz 2012

Inhalt

BUSE HEBERER FROMM
RECHTSANWÄLTE · STEUERBERATER PARTG

INTARGIA

1 Einleitung

Datenschutzmanagement – Kritischer Erfolgsfaktor für Ihr Unternehmen

Angesichts des rasanten Fortschritts der Datenverarbeitung und des damit einhergehenden Bedeutungsanstiegs des technisch-organisatorischen sowie des normativen Datenschutzes sind insbesondere zwei Triebkräfte zu erkennen: Sich immer schneller beschleunigende technische Entwicklungen und damit verbundene Ubiquität von Informationen und IT-Systemen, zunehmende staatliche Verschärfung der Datenschutzanforderungen und ansteigende Cyberkrimininalität.

Vor diesem Hintergrund stellen Datenschutz und Datenschutzmanagement kritische Erfolgsfaktoren für Unternehmen und den öffentlichen Sektor dar: Datenschutz ist in den Fokus von Unternehmensführung und Unternehmenskultur gerückt. Dies nicht zuletzt wegen der stetig zunehmenden politischen Bedeutung des Datenschutzes in Deutschland und weltweit. Zuletzt hat der deutsche Gesetzgeber mit dem Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14.08.2009 dieser Entwicklung in umfassender Weise Rechnung getragen. Die angekündigte EU-Datenschutzverordnung (siehe auch das Kapitel „Ausblick – EU-Datenschutzverordnung“ auf Seite 10 dieses Leitfadens) wird diese juristische Entwicklung weiter verstärken.

Beide Regelwerke fordern unter anderem Unternehmen (als Auftraggeber) bei der Auftragsdatenverarbeitung umfassende Dokumentations- und Prüfpflichten ab.

Um Risiken im IT-Bereich und insbesondere im Datenschutz wirksam begegnen zu können, benötigen Organisationen einen geplanten, strukturierten und methodischen Ansatz. Dieser muss sowohl die Einhaltung gesetzlicher Vorgaben (Compliance) als auch die Wahrung essentieller geschäftlicher Eigeninteressen (z.B. Schutz kritischer Mitarbeiter- und Geschäftsdaten) gewährleisten.

Die Datenschutz- und IT-Sicherheits-Experten von INTARGIA Managementberatung und BUSE HEBERER FROMM Rechtsanwälte Steuerberater hoffen, Ihnen mit diesem Leitfaden einen praktischen Ratgeber zur Beantwortung Ihrer dringendsten unternehmerischen Fragen im Bereich Datenschutz an die Hand geben zu können. Unsere Experten haben für Sie intensiv die aktuellen gesetzlichen Vorgaben analysiert und und möchten Ihnen im Folgenden ein konkretes Vorgehensmodell vorstellen, das effektiv und mit Augenmaß für ein hohes Datenschutzniveau sorgt.

Vor diesem Hintergrund freuen wir uns, Ihnen diesen gemeinsamen Leitfaden präsentieren zu dürfen.

Dr. rer.pol., Dipl.-Ing. Thomas Jurisch
Geschäftsführender Gesellschafter
ISO 27001 Lead Auditor
INTARGIA Managementberatung GmbH

Stephan Menzemer
Rechtsanwalt
Wirtschaftsmediator
Partner
BUSE HEBERER FROMM
Rechtsanwälte Steuerberater
Partnerschaftsgesellschaft

Steffen Weber, M.Sc.
Partner
ISO 27001 Lead Auditor
INTARGIA Managementberatung GmbH

Tim Christopher Caesar
Rechtsanwalt
BUSE HEBERER FROMM
Rechtsanwälte Steuerberater
Partnerschaftsgesellschaft

2 Aktuelle Fälle zum Datenschutz

Die vergangenen Jahre waren für den deutschen Datenschutz Jahre der Rechtsunsicherheit und Skandale. Staatliche und private Unternehmen haben durch verschiedenste Rechtsverstöße für Aufregung gesorgt. Kundendaten wurden gestohlen und auf dem Schwarzmarkt weiterverkauft, teilweise wurden Mitarbeiter bei der Arbeit heimlich gefilmt, ihre Daten ohne Zustimmung ausgewertet. Unpräzise und teils unausgereifte Gesetze sowie eine Unterschätzung der Bedeutung der Datenschutz-Compliance durch die Geschäftsführungen haben diese Entwicklung befördert.

Die Deutsche Bahn beispielsweise räumte ein, in den Jahren 2002 und 2003 rund 173.000 ihrer 240.000 Mitarbeiter ohne deren Wissen „überprüft“ zu haben. Deren Daten wurden mit jenen von 80.000 Firmen abgeglichen, mit welchen die Deutsche Bahn Geschäftsbeziehungen unterhält. Diese Aktion „Babylon“ sollte Korruptionsfälle im Unternehmen aufdecken. In etwa 100 Fällen („Erfolgs-“ quote von weniger als 0,2 %) haben sich Hinweise auf Korruption ergeben. Politiker geißelten dieses Vorgehen später als „Massendatenabgleich“ und „Rasterfahndung“; Anfang des Jahres 2009 trat Bahnchef Mehdorn zurück.

Mit dem Verkauf von sensiblen Kundendaten zu Lasten der Deutschen Telekom startete 2006 eine Serie von medialer Berichterstattung über Datenschutzmissbrauch. In Bonn kamen 2006 rund 17 Millionen Datensätze zu Mobilfunkprofilen abhanden. Nach dem Diebstahl wurden die Daten im Internet illegal zum Kauf angeboten. Aufsehen erregte die Affäre auch deshalb, weil geheime Nummern und Privatadressen bekannter Politiker, Wirtschaftsprüfer, Prominenter und Milliardäre entwendet wurden. Die Sicherheitsvorkehrungen des Unternehmens versagten weitgehend. Dieser „Datenklauskandal“ potenzierte sich zum „Datenspitzelskandal“. Im Unternehmen wurden Telefonverbindungsdaten von Mitarbeitern und Journalisten heimlich ermittelt und intern verwendet. Eine breite Öffentlichkeit forderte daraufhin den Rücktritt des Vorstandsvorsitzenden René Obermann.

Im Sommer 2009 stellte sich heraus, dass die Deutsche Post zum Zweck der internen Personalpolitik sensible Krankheitsdaten sammelte. Es seien Krankheitsbilder von Mitarbeitern systematisch erfasst, kategorisiert und anschließend mit Handlungsempfehlungen verbunden worden, berichtete unter anderem die FAZ. So sollten Beschäftigte „incentiviert“ werden, vorzeitig in den Vorruhestand zu gehen oder ihr Tätigkeitsfeld zu wechseln.

Auf globaler Ebene sorgte 2011 der Hackerangriff auf das Playstation Network der Sony Playstation für große mediale Aufmerksamkeit. Im Zuge des Angriffes wurden Datensätze von 77 Millionen Kunden entwendet. Die Daten reichten von Namen über Anschriften bis teilweise zu den Kreditkartendaten. Die Folge des Hackerangriffes war ein massiver Imageverlust der Marke.

Vor dem Hintergrund der Aktivitäten von Gruppen wie Anonymus dürften die bekannt gewordenen Vorfälle der vergangenen Jahre übrigens nur die (sichtbare) Spitze des Eisberges darstellen und sich zudem in Zukunft stark mehren.

Reaktion der Politik

Auf einem am 04.09.2008 durch die Bundesregierung einberufenen Datenschutzgipfel kündigte der Bundesinnenminister in Absprache mit der Bundesjustizministerin ein Gesetzespaket für Wirtschaft

und Verbraucherschutz an. Eckpunkte des Pakets waren ein „Datenschutzauditgesetz“ und die Einführung der Rechtsfigur des „Permission Marketing“ in das deutsche Wettbewerbs- und Datenschutzrecht. Dieses erlaubt die Datenweitergabe für Werbezwecke nur nach der Einwilligung der Betroffenen. In der letzten regulären Sitzung der Legislaturperiode 2009 beschloss der Bundestag die angekündigten Änderungen des Bundesdatenschutzgesetzes. Der Bundesrat legte keinen Einspruch gegen das nicht zustimmungspflichtige Gesetz ein, so dass es (in Teilen) bereits zum 01.09.2009 bzw. im Hinblick auf manche Änderungen im Laufe des Jahres 2010 in Kraft trat. Das sogenannte „Auditgesetz“ scheiterte, es wurde nie verabschiedet.

§

Die beschlossenen gesetzlichen Neuerungen im Bundesdatenschutzgesetz haben weitreichende Konsequenzen für die Geschäftspraxis der Unternehmen.

Darstellung wesentlicher Neuerungen des BDSG durch die Reform anhand ausgewählter Beispielsfälle

Die beschlossenen gesetzlichen Neuregelungen haben nach wie vor weitreichende Konsequenzen für die Geschäftspraxis der Unternehmen und erzeugen Handlungsbedarf, um das IT-Risikomanagement den neuen rechtlichen Rahmenbedingungen anzupassen, Rechtsstreitigkeiten und strafrechtliche Konsequenzen zu vermeiden und negativer Publicity vorzubeugen.

1 | In § 28 BDSG wurde neu geregelt, wann und wofür personenbezogene Daten verwendet werden dürfen. Das kompliziert strukturierte System der vorangegangenen Fassung wurde substantiell vereinfacht. § 28 II und III BDSG formulieren trennscharfe Fallgruppen, unter welchen die Übermittlung oder Nutzung von Daten zu bestimmten Zwecken zulässig ist. Nach § 28 III BDSG ist die Verarbeitung oder Nutzung von Daten grundsätzlich nur mit Einwilligung des Betroffenen möglich. Nicht sensible Listendaten dürfen unter bestimmten Ausnahmen auch ohne Einwilligung für Werbezwecke verarbeitet oder genutzt werden. Als sog. Listenmerkmale kommen z.B. Berufs-, Branchen- oder Geschäftsbezeichnung, Name, Titel, akademischer Grad, Anschrift oder das Geburtsjahr in Frage, hingegen nicht Telefonnummer oder E-Mail-Adresse. Keiner vorherigen Zustimmung des Betroffenen im Hinblick auf Verarbeitung und Nutzung bedürfen dabei die folgenden privilegierten Ausnahmetatbestände:

- **Eigenwerbung,** wobei die Listendaten (andere Daten dürfen ergänzend gespeichert werden) beim Betroffenen oder aus allgemein zugänglichen Verzeichnissen erhoben worden sein müssen,
- **Geschäftliche Werbung an eine Geschäftsadresse,**
- **Werbung** für **steuerbegünstigte Spenden,**
- **„Beipackwerbung“** und **„Empfehlungswerbung“,** solange der Absender für den Empfänger als verantwortliche Stelle eindeutig erkennbar bleibt.

2 | Ein Unternehmen darf nach § 28 III b BDSG den Abschluss eines Vertrages nicht von der Einwilligung des Betroffenen in die werbliche Verwendung seiner Daten abhängig machen („absolutes Koppelungsverbot“), wenn diesem ein anderer Zugang zu gleichwertigen Leistungen nicht oder nicht in zumutbarer Weise möglich ist.

3 | Im Hinblick auf die Auftragsdatenverarbeitung wurde auch § 11 BDSG neu formuliert. Der Auftrag ist schriftlich zu erteilen und muss dem detaillierten Anforderungskatalog des § 11 II BDSG entsprechen. Insbesondere müssen genaue Details zum Auftrag, zur Erhebung, Speicherung, Verarbeitung, Verwendung und Löschung im Auftrag enthalten sein.

4 | Seit Jahren fordern die Arbeitnehmervertretungen in Deutschland ein spezielles „Arbeitnehmerdatenschutz-Gesetz“ (siehe zuletzt Bundestagsdrucksache 17/4230). § 32 BDSG geht bereits in diese Richtung und greift die bisherige Rechtsprechung des Bundesarbeitsgerichts und Bundesgerichtshofs auf. Mitarbeiterdaten dürfen danach zukünftig nur aus folgenden Gründen für den Zweck der Abwicklung des Beschäftigungsverhältnisses erhoben, verarbeitet und genutzt werden:

- Soweit dies für **die Entscheidung über die Begründung, für die Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist,** oder
- soweit dies zur **Aufdeckung von Straftaten** bei begründetem Verdacht einer im Arbeitsverhältnis begangenen Straftat erforderlich ist, und
- wenn **schutzwürdige Interessen des Betroffenen nicht überwiegen** (letztlich Abwägung des Gerichts im konkreten Einzelfall).

Schließlich soll nach der Gesetzesbegründung § 28 I BDSG im Beschäftigungsverhältnis grundsätzlich keine Anwendung mehr finden. Ein eigenständiges Arbeitnehmerdatenschutzgesetz wird es zudem wohl nicht geben. Stattdessen sieht ein Gesetzesentwurf vor, die Vorschriften zum Arbeitnehmerdatenschutz in den §§ 32 bis 32 Buchstabe l BDSG unter dem neuen Unterabschnitt: Datenerhebung, -verarbeitung und Nutzung für Zwecke des Arbeitsverhältnisses zu regeln.

5 | Für die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen darf unter den Voraussetzungen des § 28 b BDSG ein Wahrscheinlichkeitswert für ein zukünftiges Verhalten erhoben und verwendet werden („Scoring“). Insbesondere muss das verwendete mathematisch-statistische Verfahren wissenschaftlich anerkannt sein.

6 | Die Voraussetzungen der Übermittlung von Daten an Auskunfteien werden jetzt in § 28 a BDSG geregelt. Demzufolge muss eine geschuldete Leistung trotz Fälligkeit nicht erbracht worden und die Übermittlung zur Wahrung berechtigter Interessen erforderlich sein, sowie eine weitere zusätzliche Voraussetzung der Nr. 1 bis 5 aus § 28 a I 1 BDSG vorliegen, zum Beispiel die Forderung durch ein rechtskräftiges Urteil festgestellt worden sein.

7 | Der Bußgeldkatalog des § 43 BDSG wurde erheblich erweitert und angepasst. Zum Beispiel wird der Verstoß gegen das oben genannte Koppelungsverbot geahndet. Darüber hinaus wurden die Höchstbeträge bei Bußen erhöht. Die Geldbuße soll zudem immer den Vorteil des Täters übersteigen, auch wenn dadurch der jeweilige Höchstbetrag überschritten wird.

3 Grundlagen des Datenschutzes

Im Fokus stand in der Anfangszeit (1970 gilt als das „Geburtsjahr“ in Deutschland) des Datenschutzes eher die Datensicherheit, weniger der Schutz von Personen vor Missbrauch ihrer Daten. Inbesondere die durch die damals neuartige „elektronische Datenverarbeitung EDV“ erzeugten staatlichen Datensammlungen galten als besonders wertvoll und schützenswert. Immens an Bedeutung gewann der Datenschutz in Deutschland durch das „Volkszählungsgesetz“ von 1982, das eine umfangreiche Erfassung personenbezogener Daten vorsah. Kritikpunkte wie der zu große Umfang der Fragen, der Verzicht auf die anonymisierte Befragung und Datenerhebung, sowie die Möglichkeit, die Daten zu einem umfassenden Persönlichkeitsbild zusammen zu fügen und die Weitergabe an andere Behörden, führten zu der Untersagung durch den Bundesgerichtshof. Das Urteil, das u. a. Normenklarheit, Verhältnismäßigkeit, Datensparsamkeit und Anonymisierungsmöglichkeiten fordert, schuf somit das bis heute geltende Primat der „informationellen Selbstbestimmung“, das acht Jahre später im Bundesdatenschutzgesetz (BDSG) umfassend kodifiziert wurde.

Die Politik hat seitdem immer wieder versucht, die Vorgaben des BDSG einzuschränken oder gar zu ignorieren. Bekannte Fälle sind z. B.:

- „Großer Lauschangriff“ (1998)
- „Rasterfahndung“ (2001)
- „Bundestrojaner“ (2008)

Die genannten und noch viele weitere Versuche der jeweiligen Regierungen, die gesetzlichen Vorgaben des auf das Volkszählungsurteil von 1983 zurückzuführenden Rechts auf informationelle Selbstbestimmung auszuhebeln, wurden von der Judikative für verfassungswidrig erklärt.

Personenbezogene Daten im Fokus des Schutzes

Datenschutz fokussiert, anders als IT-Sicherheit, ausschließlich personenbezogene Daten. In § 3 I BDSG heißt es dementsprechend auch „Einzelangaben oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“. Aufgeschlüsselt bedeutet dies:

- „persönlich“ – z. B. Name, Geburtsdatum, Haarfarbe etc.
- „sachlich“ – z. B. Ausbildung, Gehalt, Arbeitgeber, Wohnort etc.
- „bestimmt“ – auf die Person bezogen, z. B. ein Lohnzettel
- „bestimmbar“ – mit einem gewissen Aufwand einer Person zuzuordnen, z. B. eine IP-Adresse
- „natürlich“ – nur natürliche, keine juristischen Personen

Anforderungen an Unternehmen

Im Datenschutzrecht gelten sich teilweise ergänzende rechtliche Anforderungen, z. B. EU-Richtlinien, das Grundgesetz und das Bundesdatenschutzgesetz (BDSG). Allen Normen liegt eine übergreifende Forderung zu Grunde: Unternehmen müssen über den kompletten Informationslebenszyklus hinweg („von der Erfassung bis zur Löschung“) mit personenbezogenen Daten bewusst und sorgsam umgehen. Dabei sind insbesondere folgende Prinzipien anzuwenden:

- Verbot mit Erlaubnisvorbehalt – Die Verarbeitung ist generell verboten, es sei denn, es liegt eine Einwilligung des Betroffenen vor oder es gibt eine rechtliche Grundlage.
- Prinzip der Zweckbindung – Der Zweck der Erhebung ist bereits bei der Erhebung festzulegen und dem Betroffenen mitzuteilen.
- Prinzip der Transparenz – Es muss jederzeit nachvollziehbar sein, welche Daten des Betroffenen gespeichert, verarbeitet und gelöscht werden. Dies ist durch sog. Verfahrensverzeichnisse sicherzustellen.
- Prinzip des Direkterhebungsvorrangs – Die Erhebung von personenbezogenen Daten soll, wenn möglich, direkt beim Betroffenen erfolgen.
- Verhältnismäßigkeitsprinzip – Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten darf nur dann erfolgen, wenn dies z. B. zur Aufgabenerledigung erforderlich ist.
- Prinzip der Datensparsamkeit – Personenbezogene Daten sollten nur dann verarbeitet werden, wenn dies unbedingt erforderlich ist. Daten dürfen keinesfalls auf Vorrat gespeichert werden.

Über die genannten allgemeinen Prinzipien hinaus gelten auch explizite **Datenschutzrechte** von Betroffenen, insbesondere:

- Auskunftsrecht
- Benachrichtigungsrecht
- Berichtigungsrecht
- Löschungsrecht und Sperrungsrecht
- Anrufungsrecht
- Schadensersatzrecht

Des Weiteren wurden **Kontrollinstanzen** geschaffen:

- Die vorgenannten Betroffenenrechte stellen die sog. **Selbstkontrolle** dar.
- Die sog. **Eigenkontrolle** verpflichtet Unternehmen darüber hinaus, eine eigene Kontrollinstanz zu schaffen, den betrieblichen Datenschutzbeauftragten.
- Die sog. **Fremdkontrolle** schließlich wird durch die Aufsichtsbehörden (Landes- und Bundesdatenschutzbeauftragte mit ihren Mitarbeitern) wahrgenommen.

Darüber hinaus werden in § 9 BDSG (und dessen Anlage) konkrete **technische und organisatorische Maßnahmen** der Unternehmen zur Gewährleistung von Datenschutz gefordert. Diese umfassen die Bereiche:

- Zutrittskontrolle – Zutritt zu Gebäuden oder Räumen
- Zugangskontrolle – Zugang zu IT-Systemen
- Zugriffskontrolle – Zugriff auf Daten
- Weitergabekontrolle – Schutz von Daten beim Transport
- Eingabekontrolle – Überprüfbarkeit von Dateneingaben
- Auftragskontrolle – Weisungskontrolle bei Auftragsdatenverarbeitung
- Verfügbarkeitskontrolle – Schutz gegen zufällige Zerstörung oder Verlust von Daten
- Datentrennungskontrolle – Getrennte Verarbeitung von zu unterschiedlichen Zwecken erhobenen Daten

Vorteile für Unternehmen durch proaktiven Datenschutz

Proaktiver Datenschutz bietet jedoch weit mehr als die reine Erfüllung von Compliance-Anforderungen: Eine prozess- und organisationsbezogene Betrachtung des Datenschutzes führt zu Transparenz, der Vermeidung von nachgelagerten Kosten durch nicht datenschutzkonforme Prozesse, Anwendungen oder Systeme, sowie zu sensibilisierten Mitarbeitern. Des Weiteren trägt Datenschutz explizit zur Risikominimierung bei. Schließlich wird Datenschutz heutzutage häufig auch als Marketingaspekt genutzt.

4 Ein Ansatz für ganzheitliches, zertifiziertes Datenschutzmanagement mit Augenmaß

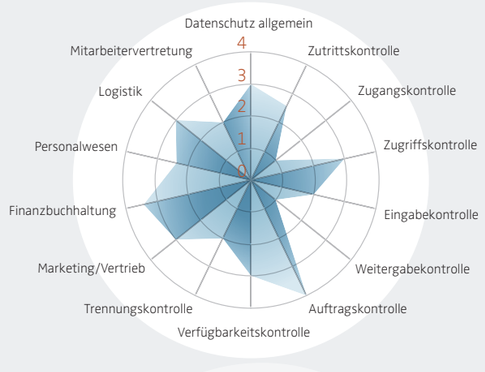
Nachhaltigkeit und Effektivität können sich nur durch einen geplanten, systematischen und zyklischen Prozess einstellen. Aus diesem Grund ist auch für den Datenschutz ein Managementsystem mit den Elementen „Planen, Durchführen, Kontrollieren, Handeln" sinnvoll.

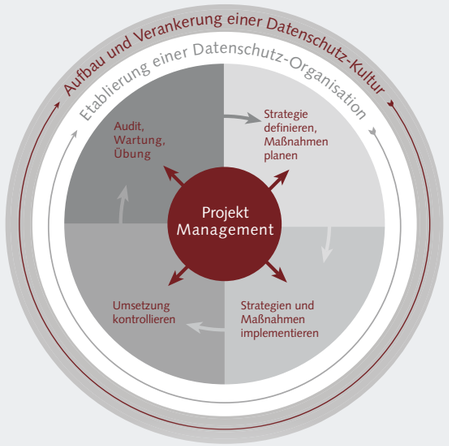
> **Phase 1: Ist-Analyse**
Zu Beginn werden mit einem Initial-Audit Maßnahmen untersucht (als „Datenschutz-Quick-Check" auch losgelöst vom Datenschutzmanagementsystem einsetzbar, um schnell und kostengünstig den Status Quo des Datenschutzes zu ermitteln). Basis der Untersuchung sind die Geschäftsprozesse des Unternehmens, in welchen personenbezogene Daten erhoben und verarbeitet werden.

Das Audit wird mit Hilfe einer professionellen, softwaregestützten Auditsoftware durchgeführt. Die Angaben der Gesprächspartner werden im Audit durch ausgewählte Stichprobenprüfungen validiert. Neben der Unternehmens-IT werden wegen ihrer Wichtigkeit für den Datenschutz immer auch das Personalwesen (Mitarbeiterdaten), Marketing/Vertrieb (Kundendaten) und der Einkauf (Lieferantendaten) separat untersucht. Im Auditbericht werden alle Untersuchungsergebnisse und Handlungsempfehlungen nachvollziehbar aufgeführt, unter anderem durch ein verständliches Ampelsystem.

> **Phase 2: Strategie definieren und Maßnahmen planen**
Im Rahmen der Ergebnisbesprechung wird die Datenschutzstrategie definiert (z. B. welches erkannte Problem bis wann zu beseitigen ist, welche Unternehmensteile Priorität haben etc.). Auf dieser Basis wird eine bedeutungsgerechte Maßnahmenplanung inklusive Priorisierung und Timeline erstellt. Da Datenschutzmanagement stets mit Augenmaß betrieben werden sollte, muss jedes Unternehmen für sich definieren, welches Niveau es anstrebt und in welchem zeitlichen Rahmen die Entwicklung erfolgen soll.

Beispielhafte grafische Darstellung des Datenschutzreifegrads nach untersuchten Bereichen.





> **Phase 3: Strategien und Maßnahmen implementieren**
Die zur Umsetzung ausgewählten Maßnahmen werden anschließend gemäß ihrer Priorisierung im Unternehmen implementiert. Die INTARGIA- und BUSE HEBERER FROMM-Datenschutzexperten stehen hier mit Expertenwissen zur Unterstützung zur Verfügung.

> **Phase 4: Umsetzung kontrollieren / Re-Audit, Wartung und Übung**
Um den wichtigen Aspekt der kontinuierlichen Verbesserung zu berücksichtigen wird in regelmäßigen Abständen das Datenschutzmanagement reauditiert (im Idealfall jährlich). Dabei können einzelne Maßnahmen angepasst und getestet sowie neue gesetzliche und sonstige Anforderungen und im Unternehmen eingetretene Veränderungen berücksichtigt werden.

> **Begleitende Aktivität 1:**
Etablierung einer Datenschutz-Organisation
Datenschutz funktioniert nur, wenn eine geeignete Organisation etabliert wird. Dazu zählt primär der Datenschutzbeauftragte als ständiger Ansprechpartner und Koordinator aller Datenschutzaktivitäten und das Projektteam, welches bei den Audits beteiligt ist. Ebenso wichtig ist aber auch das Commitment des Managements, damit der Datenschutz im Unternehmen einen hohen Stellenwert genießt.

> **Begleitende Aktivität 2:**
Aufbau und Verankerung einer Datenschutzkultur
Datenschutz kann ohne die erfolgreiche Einbeziehung der Mitarbeiter in unseren Augen keinen Erfolg haben. Als wirkungsvolle Maßnahmen haben sich z. B. Datenschutzschulungen, Sensibilisierungsveranstaltungen, regelmäßige Datenschutznewsletter bzw. die Herausgabe eines Datenschutzhandbuchs bewährt.

Zertifizierter Datenschutz

Zertifizierte Managementsysteme spielen im Wettbewerb eine zentrale und immer wichtigere Rolle, denn Unternehmen und öffentliche Einrichtungen müssen ihre Compliance-Konformität vermehrt als Verkaufsargument nutzen Organisationen, die das INTARGIA-Datenschutzmanagementsystem einsetzen und einen bestimmten Gesamtreifegrad erreichen, erhalten von INTARGIA das in Zusammenarbeit mit dem TÜV entwickelte INTARGIA-Datenschutzsiegel. Damit kann gegenüber Kunden, Mitarbeitern, Behörden und Wettbewerbern signalisiert werden, dass Datenschutz ein erfolgskritischer Faktor ist und ernst genommen wird.

Die Vorteile für Sie:
- Professionalität durch eine neutrale und praxiserprobte Datenschutzberatung
- Kenntnis über die eigene Datenschutzsituation
- Erkennung von potentiellen Geschäftsrisiken und Expertenvorschläge für deren Beseitigung
- Schaffung von Vertrauen bei Kunden, Mitarbeitern und Lieferanten
- Werbewirksames Marketinginstrument
- Nachhaltige Verbesserung der internen Prozesse und Strukturen

Kundenstimmen

Dr. Stefan Müller, Vorstand, expert AG
„2008 hat sich expert entschieden, das Thema Datenschutz mit externer Expertenunterstützung weiter zu professionalisieren. INTARGIA hat uns in einem ersten Schritt, dem Datenschutz-Quick-Check, Optimierungspotenziale aufgezeigt und mit uns gemeinsam aus diesen Handlungsempfehlungen sinnvolle und effektive Maßnahmen abgeleitet. Wir haben uns anschließend entschieden, das Amt des Datenschutzbeauftragten an INTARGIA zu geben und gemeinsam mit INTARGIA alle Maßnahmen ganzheitlich in einem Datenschutz-Management-System (DSMS) zu bündeln. INTARGIA stand uns bei der Entwicklung und Implementierung dieses DSMS und seiner Maßnahmen beratend zur Seite. Ein wichtiges Element des expert-Datenschutzmanagement-Systems sind für uns die jährlichen Re-Audits durch INTARGIA, die den Fortschritt und den jeweiligen Reifegrad des DSMS ermitteln und der Geschäftsführung transparent machen. Mittlerweile haben wir mit Hilfe von INTARGIA einen sehr hohen Datenschutzreifegrad erreicht, der u. a. auch in der Vergabe des INTARGIA-/TÜV-Datenschutzsiegels an uns dokumentiert ist. Wir haben INTARGIA in den letzten Jahren als kompetenten und zuverlässigen Partner erlebt, der uns stets mit der notwendigen Professionalität und Neutralität geholfen hat, noch besser zu werden."

Christina Becker, Group Compliance, BRITA GmbH
„Im Zuge der Etablierung einer Endkunden-Direktansprache durch unseren Webshop www.brita.de hat BRITA die eigenen Datenschutzaktivitäten verstärkt. Durch die neu entstandene Endkundennähe haben sich zahlreiche neue Datenschutzanforderungen für BRITA ergeben, z. B. im Rahmen von Gewinnspielen oder der Internationalisierung des Endkundengeschäfts. INTARGIA hat uns in all diesen Fragestellungen zu effektiven technischen und organisatorischen Maßnahmen in der Analyse-, Konzeptions-, und Implementierungsphase maßgeblich unterstützt. Neben der Datenschutzberatung hat BRITA bewusst auch die Funktion des Datenschutzbeauftragten extern an INTARGIA übergeben. Der externe Datenschutzbeauftragte arbeitet dabei sehr effektiv mit dem internen Group Compliance Management zusammen, so dass externes und internes Experten- und BRITA-Wissen bestmöglich kombiniert werden können. Bei all diesen Aktivitäten haben wir INTARGIA als fachlich überzeugenden und stets zuverlässigen Partner kennengelernt."

5 Fragestellungen aus der Praxis

Privatnutzung

Die Privatnutzung des Internets am Arbeitsplatz beschäftigt seit geraumer Zeit die Gerichte. Dieser Aspekt des Arbeitslebens ist aus arbeitsrechtlicher Perspektive vor allem deswegen brisant, weil auf eine exzessive Internetnutzung durch den Arbeitnehmer oft die Kündigung folgt. Nach einer Studie des Internet-Informationsdienstes Heise nutzt fast die Hälfte der in Deutschland tätigen Arbeitnehmer das Web am Arbeitsplatz zu privaten Zwecken für mehr als drei Stunden pro Woche. Durch die Rechtsprechung der Arbeitsgerichte, hat sich im Arbeitsrecht im Wege einer Fallrechtsbildung weitgehende Rechtssicherheit eingestellt. Im Datenschutzrecht hingegen ist das Phänomen der Privatnutzung durch Arbeitnehmer unvollständig geregelt und die anwendbaren Normen hängen vom jeweiligen Einzelfall ab.

In der datenschutzrechtlichen Praxis sind vor allem drei Konstellationen zu unterscheiden: **(I.)** Der Arbeitgeber erlaubt die private Nutzung von E-Mail und Internet, **(II.)** der Arbeitgeber verbietet die private E-Mail und Internetnutzung sowie **(III.)** der Arbeitgeber verbietet im Grundsatz die private IT-Nutzung, diese erfolgt jedoch in der täglichen betrieblichen Praxis („Duldungsproblematik").

I. Der Arbeitgeber erlaubt die private Nutzung von E-Mail und Internet.

Der Arbeitgeber hat an sich die Wahl, ob er seinen Beschäftigten die Nutzung von E-Mail und Internet zu privaten Zwecken gestatten will. Denn bei Computern und den genannten Diensten handelt es sich um betriebliche Mittel, auf deren (private) Nutzung durch den Arbeitnehmer kein Anspruch besteht. Wenn und soweit der Arbeitgeber seinen Beschäftigten die private Internetnutzung gestattet, ist er allerdings an das Fernmeldegeheimnis nach § 88 TKG gebunden. Lediglich soweit es zum Zwecke der Bereitstellung, Abrechnung und Sicherstellung eines geregelten Kommunikationsablaufes notwendig ist, dürfen Userdaten dann noch erfasst und verwendet werden. Daher sollte immer eine passende Regelung der Privatnutzung implementiert werden.

In dem geschilderten Szenario ist der Arbeitgeber zudem sogar Anbieter von Telemedien im Sinne des Telemediengesetzes (TMG). Wegen des dann bestehenden Anbieter-Nutzer-Verhältnisses, ist der Arbeitgeber verpflichtet, die Datenschutzbestimmungen des TMG zu beachten. Insbesondere ist hier § 15 TMG hervorzuheben, nach dem der Arbeitgeber die so genannten Nutzungsdaten eines Users nur dann erheben und verwenden darf, wenn dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (§ 15 I TMG). Als Nutzungsdaten im Sinne des Gesetzes gelten insbesondere Merkmale zur Identifikation des Users, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien. Nicht gestattet ist dem Arbeitgeber übrigens im Grundsatz die Erfassung von Anbieter, Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von einem Nutzer in Anspruch genommener Telemedien auf der Abrechnung, es sei denn, der Arbeitnehmer verlangt im Einzelfall ausnahmsweise einen Einzelnachweis (z.B. bei Belastung des Arbeitnehmers mit hohen privaten Telefonkosten durch den Arbeitgeber).

II. Der Arbeitgeber verbietet die private E-Mail- und Internetnutzung.

Wenn der Arbeitgeber die private Nutzung von Internet und E-Mail durch die Arbeitnehmer verbietet (was so strikt für die meisten Unternehmen allerdings nicht in Betracht kommt), ist er datenschutzrechtlich besser gestellt. Im Gegensatz zu dem oben geschilderten Szenario ist der Arbeitgeber dann nämlich kein Anbieter i.S.d. TMG und TKG, mit der Folge dass diese Normen auch nicht anzuwenden sind. Weiterhin Geltung hat jedoch das BDSG. Daher ist die Erhebung und Speicherung von Internetverbindungsdaten für einen konkreten Zweck, wie etwa die Erstellung einer Abrechnung, zulässig. Nicht erlaubt ist dem Arbeitgeber aber die Kontrolle des Inhalts privater E-Mails. Insoweit entspricht die Rechtslage weitestgehend der Rechtslage in Bezug auf den Inhalt privater Telefongespräche. Ein Mitschneiden oder Mithören solcher Gespräche stellt nach der Rechtsprechung des Bundesverfassungsgerichts einen Eingriff in das allgemeine Persönlichkeitsrecht des Arbeitnehmers aus Art. 2 I in Verbindung mit Art. 1 I GG dar. Solche Eingriffe sind nach der deutschen Rechtsprechung immer nur dann zulässig, wenn der Eingriff in das allgemeine Persönlichkeitsrecht einem höherrangigen Interesse dient. Ob dies im Einzelfall zutrifft, wird letztlich durch das angerufene Gericht festgestellt. Zulässig kann ein solcher Eingriff etwa dann sein, wenn der hinreichende Verdacht besteht, dass das Verhalten des Arbeitnehmers einen Straftatbestand erfüllt. Sollte die Abwägung zu Gunsten des Arbeitnehmers ausfallen, und damit der Eingriff in das allgemeine Persönlichkeitsrecht als rechtswidrig eingestuft werden, kann dies unter anderem zur Folge haben, dass solche rechtswidrig erlangten Erkenntnisse nicht im Rahmen eines gerichtlichen Verfahrens als Beweismittel verwertet werden dürfen.

III. Die private Nutzung ist generell verboten, diese erfolgt jedoch in der täglichen betrieblichen Praxis („Duldungsproblematik").

Als Entstehungsgrund einer betrieblichen Übung wird verbreitet das „vorbehaltlose Dulden" oder „Geschehenlassen" der privaten Nutzung des Web aufgefasst. Diesbezüglich ist zu berücksichtigen, dass eine vorbehaltlose Duldung die genaue Kenntnis des zu duldenden Sachverhalts voraussetzt. Der genaue Umfang der privaten Nutzung durch den Arbeitnehmer wird dem Arbeitgeber jedoch regelmäßig gerade unbekannt sein, so dass eine vorbehaltlose Duldung durch den Arbeitnehmer schwer zu beweisen sein wird. Die Wirksamkeit des Verbots der privaten Nutzung der IT setzt daher im Grundsatz auch keine permanente Überwachung der Arbeitnehmer durch den Arbeitgeber voraus, Stichproben genügen regelmäßig. Und: Selbst bei Kenntnis des Arbeitgebers von der Privatnutzung lässt sich aus der schlichten Duldung kein Bestimmungsrecht des Arbeitnehmers im Sinne von § 315 BGB über Arbeitgeberleistungen (Umfang der Zurverfügungstellung der IT/Nutzung der IT) ableiten.

Datenschutz im Beschäftigungsverhältnis

Seit Jahrzehnten werden in Deutschland Forderungen nach einem Arbeitnehmerdatenschutzgesetz diskutiert. Die Datenschutzskandale, insbesondere bei Lidl, bei der Deutschen Telekom und der Deutschen Bahn, ließen Reaktionen der Politik unausweichlich werden. Aber entgegen den Erwartungen der Datenschützer entschied sich die Regierung für die sog „kleine Lösung" und nahm in das BDSG lediglich den neuen § 32 BDSG auf, anstatt ein spezielles Beschäftigtendatenschutzgesetz („BDatG") zu erlassen, die sog. „große Lösung". § 32 BDSG kodifizierte weitgehend die deutsche Rechtsprechung zum Arbeitnehmerdatenschutz. Die neue Regelung trat zum 01.01.2009 in Kraft. Zudem ist eine „große Lösung" nicht länger Gegenstand der politischen Diskussion. Vielmehr sollen spezifischere Regelungen nach § 32 BDSG eingefügt werden.

Erhebung der Daten nach § 32 I 1 BDSG

Personenbezogene Daten dürfen nach § 32 I 1 BDSG n. F. zum Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden. Der Begriff des Beschäftigungsverhältnisses ist dabei weiter zu verstehen als der des Arbeitsverhältnisses. Die Definition ergibt sich aus § 3 XI BDSG. Maßgeblich für die Zulässigkeit der Datenverarbeitung ist, ob die Maßnahme „erforderlich" für die Begründung, Durchführung oder Beendigung des Verhältnisses ist. Der Begriff der Erforderlichkeit ersetzt die bloße Zweckdienlichkeit des § 28 I Nr. 1 BDSG a. F. Grundsätzlich ist eine Maßnahme dann erforderlich, wenn es kein gleich geeignetes, milderes Mittel gibt, um das Ziel zu erreichen. Hierbei hat der Arbeitgeber sein unternehmerisches Interesse an der Datenerhebung mit den Grundrechten der Beschäftigten auf informationelle Selbstbestimmung abzuwägen. Das Ergebnis dieser Abwägung muss belegen, dass die Datenerhebung tatsächlich erforderlich ist. Unbedenklich sind Datenerhebungen zur Erfüllung seiner Pflichten, wie z.B. für die Personalverwaltung, die Lohn- oder Gehaltsabrechnung.

Aufdeckung von Straftaten

Ein Ziel der BDSG-Novelle war es, das „ermittlerische" Handeln der Arbeitgeber zu beschränken. Insbesondere im Visier waren „heimliche Videoüberwachungen" und „Massenscreenings" von Arbeitnehmerdaten. Nach § 32 I 2 BDSG darf der Arbeitnehmer zur Aufdeckung von Straftaten Daten erheben:

- bei begründetem Verdacht einer Straftatbegehung,
- wenn diese Erhebung erforderlich ist,
- die Interessen des Beschäftigten nicht überwiegen und
- die Maßnahme nicht unverhältnismäßig ist.

Diesbezüglich ist zu berücksichtigen, dass „Ordnungswidrigkeiten“ keine Straftaten sind. Als Straftat bezeichnet das deutsche Strafrecht eine Verhaltensweise, die durch ein Strafgesetz mit Strafe bedroht ist. Dem gegenüber ist eine Ordnungswidrigkeit eine rechtswidrige und vorwerfbare Handlung, für die das Gesetz als Ahndung nur eine Geldbuße vorsieht.

Für die Aufdeckung von Ordnungswidrigkeiten („sonstiger Complianceverstöße“) oder für die Verhinderung von Straftaten („präventive Gefahrenabwehr“) soll nach dem Willen des Gesetzgebers § 32 I 1 BDSG anwendbar sein, denn Complianceanstrengungen von Unternehmen zielen auf die Einhaltung von Gesetzen und Richtlinien ab und fallen daher nicht unter die Spezialregelung des § 32 I 2 BDSG zur Aufdeckung von Straftaten im Beschäftigungsverhältnis (konkreter Strafverdacht für Diebstahl, Korruption, etc.). Die Straftat muss außerdem beschäftigungsbezogen sein, also nicht rein privat. Tatsächliche Anhaltspunkte, die einen Verdacht begründen, müssen dokumentiert werden und da der Verdacht sich nur gegen eine geringe Anzahl von Beschäftigten richten wird, sind „Massenscreenings“ oder „Rasterfahndungen“ regelmäßig ausgeschlossen. Die Zulässigkeit einer verdeckten Videoüberwachung wird von der Zahl der Beobachteten abhängen. Die Einrichtung einer **„Whistleblower-Hotline“** soll durch die Sicherstellung der Vertraulichkeiten der Meldungen und die organisatorische Trennung der Complianceabteilung von der Personalabteilung begleitet werden. Je schwerer die Straftat wiegt und der Verdacht erhärtet ist, umso intensivere Maßnahmen sind gesetzlich erlaubt. Der sicherste Weg für den Arbeitgeber bleibt aber ein restriktives Informationsmanagement und/oder der physikalische Schutz besonders diebstahlgefährdeter Gegenstände („sog. technisch-organisatorischer Datenschutz“).

§

Vermeidung von Unklarheiten bei Umgang mit Privatnutzung der IT durch explizite Regelung im Arbeitsvertrag oder durch Betriebsvereinbarung.

Relevante Daten?

Nach § 32 II BDSG ist weder ein automatisiertes Verfahren, noch ein Dateibezug erforderlich. Somit betrifft die Norm auch Daten aus Personalakten oder aus bloßen Telefonnotizen. Diese Erweiterung findet man z.B. nicht im § 28 I BDSG.

Verhältnis zu § 28 BDSG

§ 28 I BDSG soll nach dem Willen des Gesetzgebers grundsätzlich für Zwecke des Beschäftigungsverhältnisses gesperrt sein, da § 32 BDSG die einwilligungsfreie Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten für Zwecke eines Beschäftigungsverhältnisses regelt. § 28 I Nr. 2 und 3 BDSG bleiben unter anderem für „andere Zwecke“ anwendbar (z.B. zur Durchführung einer **„Due Diligence“**). Dies ist der Fall, wenn zunächst im Rahmen des § 32 I 1 BDSG gespeicherte Daten nachträglich für andere Zwecke verwendet werden sollen. Auch die Hinweispflicht für den Empfänger übermittelter Daten in § 28 V BDSG findet weiterhin Anwendung. Für die Datenverarbeitung im Rahmen arbeitsrechtlicher Beziehungen kann darüber hinaus auch § 28 VI Nr. 3 Anwendung finden. Demzufolge können Daten erhoben, verarbeitet oder genutzt werden, soweit dies zur Geltendmachung, Ausübung oder Verteidigung von Ansprüchen erforderlich scheint und das Schutzinteresse des Betroffenen nicht überwiegt.

Ausblick – EU-Datenschutzverordnung

Die EU-Kommission plant eine grundlegende Erneuerung und in diesem Rahmen Vereinheitlichung der Datenschutzgesetze in der EU. Der bereits im Dezember 2011 vorab inoffiziell veröffentlichte und Ende Januar 2012 offiziell vorgestellte Entwurf einer EU-Datenschutzverordnung trifft bei den Experten auf ein geteiltes Echo.

Auch wir können festhalten, dass die geplanten Neuerungen in der Praxis der von uns beratenen Unternehmen sowohl Chancen als auch Erschwernisse bringen werden: Aus Compliancesicht ist die damit verbundene Modernisierung des Datenschutzrechts wie auch die mit dem rechtlichen Instrument der unmittelbar geltenden Verordnung zu erreichende Vereinheitlichung des Datenschutzrechts innerhalb der EU sehr zu begrüßen. So entsteht Klarheit und Planungssicherheit sowie insbesondere eine Erleichterung bei grenzüberschreitend tätigen Unternehmungen, die mittelfristig durch den Einsatz einer ganzheitlichen Strategie nicht zuletzt auch eine Kostenersparnis bedeuten wird.

Auch wenn deutsche Unternehmen bereits bisher mit dem Bundesdatenschutzgesetz strengeren Regelungen unterworfen waren, als manch ausländischer Konkurrent, werden durch die Verordnung hierzulande etliche Änderungen zu berücksichtigen sein: Je nachdem, was letztlich am Ende des gerade erst begonnenen Gesetzgebungsprozesses stehen wird, können sich z.B. zusätzliche Erfordernisse im Hinblick auf Dokumentations- und Informationspflichten, das umstrittene „Recht auf Vergessenwerden“ oder die Datenportabilität ergeben.

Bis zum Inkrafttreten der potentiellen neuen EU-Datenschutzverordnung wird sich – nicht zuletzt durch den Einfluss von Interessenverbänden und den Regierungen der EU-Staaten – noch einiges tun. Hinzu kommt, dass parallel auch in Deutschland Änderungen im Datenschutzrecht vorangetrieben werden; so nahm die bereits tot geglaubte Novelle des Beschäftigtendatenschutzes Anfang 2012 wieder Fahrt auf.

Jedes Unternehmen und jeder Unternehmer tut daher gut daran, die aktuellen und zukünftigen Entwicklungen zu berücksichtigen – nicht zuletzt, um beim Einsatz der immer wichtiger werdenden Compliance-Strategien und -Instrumente die Nachhaltigkeit entsprechender Investitionen zu sichern. Die Datenschutzexperten der Practice Group Technology von BUSE HEBERER FROMM sowie von der INTARGIA Managementberatung stehen Ihnen hierzu selbstverständlich gerne zur Verfügung.

Ausgewählte Aspekte und erste Einschätzung bezüglich Veränderungen oder Neuerungen im Datenschutzrecht durch die geplante EU-Datenschutzverordnung:

- Die Verordnung wird aufgrund ihres rechtlichen Charakters direkt ab Inkrafttreten einheitlich bindend für den nicht-öffentlichen Bereich in allen Mitgliedsstaaten sein
- Erleichterung des internationalen Datentransfers durch Harmonisierung
- Sanktionsmöglichkeiten sollen „erheblich verstärkt und effektiver ausgestaltet werden“ (Eine grundsätzliche Auflösung der Bußgeldobergrenze und Ersetzung durch Gewinnabschöpfungsmöglichkeiten ist möglich)
- IT-Verfahren sollen verpflichtend mit einer datenschutzfreundlichen Grundeinstellung („Privacy by default“) versehen werden
- Bei Einsatz von neuen IT-Verfahren und -Systemen sollen Unternehmen auf eine „Folgenabschätzung des IT-Einsatzes“ verpflichtet werden (wahrscheinlich ist, dass eine zusätzliche Dokumentationspflicht daraus entsteht)
- Datenschutz als Wettbewerbsvorteil für Unternehmen soll weiter gefördert werden
- Aktuell gültige Erlaubnistatbestände sollen teilweise durch den Grundsatz ersetzt werden, dass Datenverarbeitung generell nur mit Einwilligung zulässig ist (dadurch steigen die Anforderungen an rechtskonform und effektiv gestaltete Kundendaten-erfassungs-, -verarbeitungs- und -bewertungsprozesse)
- Betroffene sollen Ihre Rechte ohne „technisch-organisatorische Hindernisse“ nutzen können (z. B. Onlineauskunft), innerhalb eines Zeitrahmens von einem Monat
- Es sind Datenschutzarbeitsanweisungen zu erstellen („Policies“), die regeln, wann welche Daten verarbeitet werden und wie die Rechte des Betroffenen gewahrt werden (vermutlich werden hierdurch die im deutschen BDSG bereits geforderten Verfahrensverzeichnisse abgelöst)
- Erweiterung von Benachrichtigungs- und Auskunftspflichten ggü. Betroffenen, z.B.: verpflichtende Bekanntmachung des DSB; Darstellung der Begründung, warum Datenverarbeitung erfolgt, wann die Daten regelmäßig gelöscht werden und welche geplanten Drittstaatentransfers vorgesehen sind
- Nationale Beschäftigtendatenschutzregeln sind möglich
- Unternehmen mit weniger als 250 Mitarbeitern sollen von der Pflicht der Bestellung eines Datenschutzbeauftragten entbunden werden.

Kontakt und Informationen

INTARGIA

INTARGIA Managementberatung GmbH

Dr. rer. pol., Dipl.-Ing. Thomas Jurisch
Geschäftsführender Gesellschafter
ISO 27001 Lead Auditor
> thomas.jurisch@intargia.com
Telefon 06103 50860

Steffen Weber, M.Sc.
Partner
ISO 27001 Lead Auditor
> steffen.weber@intargia.com
Telefon 06103 50860

BUSE HEBERER FROMM
RECHTSANWÄLTE · STEUERBERATER PARTG

BUSE HEBERER FROMM
Rechtsanwälte Steuerberater
Partnerschaftsgesellschaft

Stephan Menzemer
Rechtsanwalt
Wirtschaftsmediator
Partner
> menzemer@buse.de
Telefon 069 971097 913

Tim Christopher Caesar
Rechtsanwalt
> caesar@buse.de
Telefon 069 971097 911

10/2012