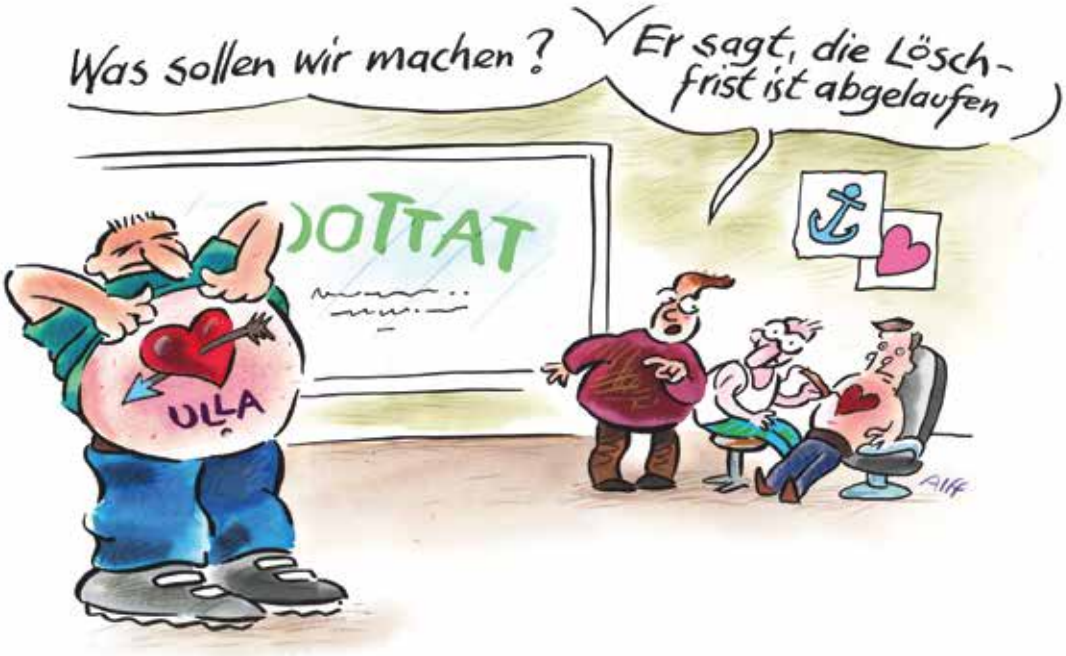

Löschen nach Regeln – die neue Norm hilft

LÖSCHFRISTEN *Wer kennt sie nicht: die ratlosen Gesichter auf Arbeitgeberseite, wenn man bei Verhandlungen über ein IKT-System nach den Löschfristen fragt. Niemand wagt zu bestreiten, dass die Festlegung einer Löschfrist für jedes personenbezogene Datum rechtlich gefordert ist. Trotzdem hakt es bei der Umsetzung meist ganz gewaltig.*

VON **VOLKER HAMMER** UND **KARIN SCHULER**

DARUM GEHT ES

1. Beschäftigtendaten müssen nach Zweckerfüllung gelöscht werden.

2. Die DIN 66398 hilft beim Entwickeln eines Löschkonzepts.

3. Löschregeln sollten Bestandteil von Vereinbarungen zu IKT-Systemen sein.

Heutige IKT-Systeme unterliegen ausnahmslos der Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG, weil sie zur Leistungs- und Verhaltenskontrolle geeignet sind. Dass dies so ist, liegt in erster Linie daran, dass sie nicht ohne Beschäftigtendaten betrieben werden können.

Gleichzeitig unterliegen Beschäftigtendaten, wie alle personenbezogenen Daten, den Regelungen des Datenschutzes. Neben Forderungen nach Zulässigkeitsgrundlage, Zweckbindung und Transparenz ist das Prinzip der Erforderlichkeit eine grundlegende Stütze datenschutzkonformer Gestaltung. Dem Erforderlichkeitsprinzip Rechnung zu tragen heißt, Daten nur zu erheben, wenn sie zur zulässigen Zweckerfüllung unbedingt nötig sind und sie auch nur solange aufzubewahren, bis der Zweck erfüllt ist. Daraus folgt unmittelbar, dass die Lebensdauer von Daten nach den Datenschutzvorschriften zeitlich begrenzt ist. Was wiederum bedeutet, dass sie nach Ablauf dieser Periode sicher gelöscht werden müssen.

Die Rechtslage

Das Bundesdatenschutzgesetz (BDSG) und andere Datenschutzgesetze fordern, dass Daten gelöscht werden, »... sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung

nicht mehr erforderlich [ist]« (§ 35 Abs. 2 Nr. 3 BDSG).

Betriebs- und Personalräten scheint diese Tatsache oft klarer vor Augen zu stehen als den Arbeitgebern, die die Pflicht zur Organisation der Löschung trifft. Es scheint so viel einfacher, Daten in großem Umfang zu sammeln, als deren Löschung sachgerecht und wohlüberlegt zu organisieren.

Betriebsvereinbarungen sind nicht nur Ausdruck ausgeübter Mitbestimmung. Sie können aus Sicht des BDSG auch eine Rechtsgrundlage sein, nach der der Arbeitgeber Beschäftigtendaten im IKT-System überhaupt erst verarbeiten darf. Wird der Zweck in einer solchen Vereinbarung ausreichend präzise beschrieben, ergibt sich auch, wann er erfüllt ist. Die Daten müssen anschließend gemäß BDSG gelöscht werden. Damit kommt derartigen Vereinbarungen für die Löschpflicht eine wichtige Rolle zu: Sie begründen nicht nur die Bedingungen für die Erhebung und den Gebrauch von Beschäftigtendaten, sondern auch deren geregelte Löschung und damit den Schutz vor dem Missbrauch gehorteter und unnötiger Altdaten.

Zahlreiche Vereinbarungen zu IKT-Systemen enthalten Anlagen, in denen Löschfristen benannt werden oder sogenannte Löschkonzepte hinterlegt sind. Deren Inhalte lösen jedoch nur selten den hohen Anspruch ein, den die Überschrift suggeriert. Aber was ist eigentlich so schwierig an Löschfristen?

Das Problem

Zur offensichtlich hohen Hürde des Löschens tragen mehrere Probleme bei.

Beginnen wir mit mentalen Widerständen. Zum einen sind Mitarbeiter aller Ebenen unsicher, was wohl passieren mag, wenn man Daten löscht. Dazu liegen in der Regel keine Erfahrungen vor. Da auch die Dokumentation von Software diese Funktion meist beschweigt, wird unterschwellig befürchtet, dass IKT-Prozesse gestört werden oder dass bestimmte Abläufe oder Auswertungen nicht mehr möglich seien. Solche Schwierigkeiten können tatsächlich eintreten, wenn die Löschung nicht sorgfältig vorbereitet wird.

Zum anderen können sich Arbeitnehmer von ihren Datenbeständen nicht lösen, weil vage erwartet wird, dass die Daten ja noch gebraucht werden könnten. Derartig unbestimmte Zwecke sind nach dem BDSG nicht zulässig, denn das Vorhalten solcher Daten wäre als Vorratsdatenspeicherung einzustufen. Wären die Zwecke dagegen bekannt, beispielsweise konkrete statistische Auswertungen, dann könnte man die Verarbeitung auch gleich durchführen und nur die Ergebnisse aufbewahren, die Rohdaten aber löschen. Der Widerstand beruht in solchen Fällen meist darauf, dass die Auswertungserfordernisse nicht klar benannt werden.

Oft verhindern auch technische Hindernisse, dass Daten gelöscht werden. Wenn IKT-Prozesse auf komplexe Weise zusammenwirken, sind auch die Techniker manchmal nicht mehr in der Lage, die Konsequenzen von Löschungen zu überschauen. Dies ist in der Regel ein klares Signal dafür, dass man Know-how aufbauen und Systeme möglicherweise entkoppeln sollte. Denn vergleichbare Abhängigkeiten bestehen auch im Regelbetrieb und Know-how hilft bei jeder Art von Störung, einen ordnungsgemäßen Betrieb wiederherzustellen. Mangelndes Verständnis ist keine Entschuldigung für den Verzicht auf Löschen.

Zu den technischen Hindernissen zählt ebenso, dass in zahlreichen Systemen gar keine Löschmechanismen vorgesehen sind. Manchmal lässt sich zwar auf »Umwegen« löschen – aber dann werden Störungen wahrscheinlicher oder der Hersteller lehnt Wartung oder Service ab. Wenn Löschen deshalb unterbleibt, trägt das Risiko des Gesetzesverstoßes immer die verantwortliche Stelle, nicht etwa der Hersteller der Software.

Schließlich ist es häufig schwierig, die fachlichen Zusammenhänge zu überschauen. Wenn gleiche Daten in mehreren Prozessen zu unterschiedlichen Zwecken verwendet werden, führt dies meist zu einer sehr komplexen Verzahnung organisatorischer Abläufe und zugehöriger IKT-Anwendungen. In der Folge gibt es möglicherweise niemanden, der sicher bestimmen kann, wann sämtliche beteiligte Prozesse beendet sind und die Daten demzufolge gelöscht werden könnten.

Die dargestellten Schwierigkeiten führen dazu, dass sowohl auf der fachlichen als auch auf der übergeordneten betriebsorganisatorischen Ebene Löschen als Aufgabe oft gar nicht erst betrachtet wird. Es verwundert nicht, dass in solchen Fällen Systeme beschafft oder entwickelt werden, auch wenn sie keine angemessenen Löschfunktionen bereitstellen.

Löschen ist nicht einfach. Trotzdem stellen die aufgeführten Schwierigkeiten keine Recht-

HINTERGRUND

DIN 66398: Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Beuth-Verlag

Eine Übersicht zu den Inhalten der Norm und einige weiterführende Hinweise gibt außerdem die Website: **www.DIN-66398.de**

LESETIPPS

Fraenkel / Hammer: Rechtliche Löschvorschriften, in: DuD 12/2007, 899 ff., Download unter: **www.secorvo.de** > Publikationen > Fachartikel > 2007

Hammer / Fraenkel: Löschklassen – standardisierte Fristen für die Löschung personenbezogener Daten, in: DuD 12/2011, 890 ff., Download unter: **www.secorvo.de** > Publikationen > Fachartikel > 2011

Hammer / Schuler: Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, 2012 (dieses Dokument ist eine Vorversion der Norm), Download unter: **www.secorvo.de** > Publikationen > Fachartikel > 2012

Fraenkel / Hammer: Erfahrungen bei der Umsetzung eines Löschkonzepts, in: DANA 1/2013, 8 ff., Download unter: **www.secorvo.de** > Publikationen > Fachartikel > 2013

fertigung zum Gesetzesbruch dar. Sowohl Datenschutzgesetze als auch Betriebsvereinbarungen sind einzuhalten. Löschen ist also Pflicht. Damit alle Datenbestände gleichermaßen korrekt gelöscht werden, bedarf es einer systematischen Vorgehensweise. Diese muss dokumentiert werden, und zwar sinnvollerweise in einem Löschkonzept für das Unternehmen.

Die Lösungsidee: Eine Norm lehrt das Löschen

Wie lange muss eine Personalakte eigentlich aufbewahrt werden, nachdem der Mitarbeiter ausgeschieden ist? Und wie lange bleiben alte Bankverbindungen der Mitarbeiterin im Abrechnungssystem, nachdem sie zu einer neuen Bank gewechselt ist? Auf Fragen dieser Art bekommt man nicht selten ratlose Gesichter zu sehen.

Hat man sich durchgerungen, nicht mehr erforderliche Daten löschen zu wollen, so stellt man meist fest, dass es keine systematische Kenntnis über Aufbewahrungsfristen und daraus resultierende Löschfristen gibt. Die erste und häufig größte Hürde bei Projekten zum Löschen von Daten ist daher, dass schlicht keine Löschregeln existieren. Ohne diese können jedoch keine Löschmechanismen implementiert und konfiguriert werden. Und genau an dieser Stelle gibt die neue DIN 66398 Hilfestellung: Sie ist eine »Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten«. Sie führt ein Unternehmen also schrittweise durch die Abläufe, die bis zur korrekten Löschung personenbezogener Daten nötig sind.

Löschregeln können von Unternehmen zu Unternehmen sehr unterschiedlich aussehen: Jede verantwortliche Stelle unterliegt möglicherweise speziellen Rechtsvorschriften, hat ihre eigenen Betriebsvereinbarungen und ihre spezifischen Datenbestände. Auch wenn sich bestimmte Betriebsabläufe und ihre Rechtsgrundlagen in vielen Unternehmen ähneln, so ergeben sich doch zahlreiche Abweichungen im Detail.

Beispielsweise lässt sich aus den Vorgaben des Allgemeinen Gleichbehandlungsgesetzes ableiten, dass man Bewerberdokumente für mindestens zwei Monate nach Aussendung einer Ablehnung aufbewahren darf, um bei in diesem Zeitraum erhobenen Klagen Nachweis führen zu können. Daher werden viele Unternehmen in Bezug auf Bewerberdaten ähnliche Löschfristen definieren. Zusätzlich können aufgrund betriebsspezifischer Abläufe oder Anforderungen spezielle Löschregeln notwendig sein. Betreibt das Unternehmen beispielsweise mit Einwilligung der Betroffenen einen Bewerberpool für spätere Stellenausschreibungen, dann muss die allgemeine Löschregel (»nach zwei Monaten«) ergänzt werden (»wenn eine Einwilligung vorliegt, dann für den zugestimmten Zeitraum«).

Die DIN 66398 kann deshalb keine allgemein geltenden Löschregeln festlegen. Sie beschreibt aber, welche Elemente ein Löschkonzept enthalten sollte und vermittelt dadurch eine klare Vorstellung davon, welche Aufgaben für systematisches Löschen erledigt werden müssen. Sie schlägt eine Vorgehensweise vor, mit der Löschregeln auf effiziente Weise definiert werden können. Diese Vorgehensweise kann für alle Arten von Daten angewandt werden, also auch für die Daten von Beschäftigten.

Das Vorgehen ist außerdem praxiserprobt: Die Norm entstand aus den Erfahrungen mit Entwicklung und Einsatz eines umfassenden Löschkonzepts bei der Toll Collect GmbH, der Betreiberin des deutschen Mautsystems. Die Unternehmen Blancco, Datev, Deutsche Bahn, Secorvo und Toll Collect fanden diese Vorgehensweise überzeugend und förderten in einem Normungsprojekt die Weiterentwicklung der »Leitlinie Löschkonzept« zur DIN 66398. Die Norm wurde im September 2015 verabschiedet und kann von allen Unternehmen angewandt werden.

Der Kern der Norm beschreibt ein Verfahren, wie auf effiziente Weise Löschregeln gefunden werden können. Dazu werden zunächst sogenannte Datenarten identifiziert. Eine Datenart umfasst die Daten, die zu einem einheitlichen Zweck verwendet werden. Beispiele für Datenarten sind: Kommen-/Gehen-Zeiten, Anmelde-Protokolle, Mitarbeiter-Stammdaten, Gehaltsabrechnungen, Reisekostenabrechnungen oder auch Abmahnungen. Die Form der Speicherung, also beispielsweise auf Papier, in einer Datenbank oder auf CD, spielt dabei keine Rolle.

Sodann sollen Löschklassen gebildet werden, in denen die Datenarten gruppiert werden können. Hierdurch wird die Komplexität verringert und die spätere Umsetzung vereinfacht. Die Gruppierung orientiert sich an wenigen Standardlöschfristen. Es gibt außerdem drei unterschiedliche Startzeitpunkte für die Stan-

MATRIX VON LÖSCHKLASSEN (BEISPIEL: TOLL COLLECT)

Startzeitpunkte \ Standardlöschfristen	sofort	42 Tage	120 Tage	1 Jahr	4 Jahre	7 Jahre	12 Jahre
Erhebung			Mautdaten	Mautdaten mit besond. Analysebedarf			
Ende des Vorgangs	Web-Logs, nmF	Kurzzeitdokumentation, Betriebs-Logs	Voll erstattete Reklamationen	Vorgänge ohne Dokumentationspflicht	Reklamations- und Forderungsdaten	Handelsbriefe	Buchhaltungsdaten
Ende der Beziehung zum Betroffenen				ergänzende Stammdaten		Verträge	Kernstammdaten

Eine Spalte der Matrix steht für eine Standardlöschfrist; die Frist stammt je nach Hintergrund aus:
allgemeinen Gesetzen spezifischen Gesetzen für die verantwortliche Stelle frei gewählt

dardlöschfristen. Werden die Standardlöschfristen und die Startzeitpunkte kombiniert, entsteht die Matrix der Löschklassen (siehe die Abbildung oben). Jede Zelle der Matrix repräsentiert eine Löschklasse mit einer Standardfrist und einem Startzeitpunkt.

Jede Datenart wird in eine Zelle dieser Matrix eingeordnet und erhält dadurch ihre Löschregel. Datenarten mit ähnlichen Zwecken stehen somit in der Matrix in der gleichen Zelle. So lässt sich gut beurteilen, ob Datenbestände für ähnliche Zwecke auch auf gleiche Weise gelöscht werden. Nachdem alle Datenarten so eingeordnet wurden, liegt ein Katalog von Löschregeln für die verantwortliche Stelle vor.

Die in der Norm beschriebene Vorgehensweise hat zwei große Vorteile: Löschregeln können in den meisten Fällen sehr schnell festgelegt werden und gleichzeitig erhalten sie eine übersichtliche Struktur. Das erleichtert das Verständnis bei allen Beteiligten: Fachabteilungen, Datenschutzbeauftragte, IT-Administratoren, Entwickler und nicht zuletzt bei Betriebs- oder Personalräten.

Die Umsetzungsvorgabe für ein System kann dann erstellt werden, indem die Datenarten identifiziert werden, die im System gespeichert werden. Zu diesen Datenarten werden die Löschregeln im Katalog herausgesucht. Auf dieser Basis werden die konkreten Mechanismen (zum Beispiel automatisch/manuell, Häufigkeit, Verantwortliche) festgelegt, die die Löschung umsetzen. Umsetzungsvorgaben können in eigenständigen Dokumenten niedergelegt sein. Es ist aber möglich, sie in eine bereits bestehende Dokumentenlandschaft, beispielsweise in Betriebshandbücher, zu integrieren.

Vereinbarung als Motor

Betriebsvereinbarungen können als Ergebnis eines Mitbestimmungsprozesses über IKT-Systeme auch den Umgang mit Beschäftigtendaten regeln. Sie sind daher auch ein gutes Mittel, um zu steuern, wie Beschäftigtendaten gelöscht werden. Es kann in der Betriebsvereinbarung allerdings nicht darum gehen, die erforderliche technische Dokumentation statt in der IKT-Abteilung nun in der Vereinbarung abzulegen. Vielmehr müssen die aus Mitbestimmungssicht wesentlichen Teile der IKT-Dokumentation in geeigneter Form als Anlage der Vereinbarung beigefügt werden.

Würden Löschregeln originär in den Betriebsvereinbarungen festgelegt, zerfiele der Katalog der Löschregeln auf mehrere oder viele Dokumente und die Konsistenz zwischen Betriebsvereinbarung und IKT-Dokumentation wäre gefährdet.

Mit Blick auf die Empfehlungen der Norm ist eine andere Strategie möglich und empfehlenswert: Verständigt man sich auf eine modulare Betriebsvereinbarungsstruktur oder besteht eine solche bereits, dann lassen sich Querschnittsthemen gewissermaßen vor die Klammer ziehen und in einer Grundlagenvereinbarung regeln. So wie sich rechtskonforme

DIN 66398

Weitere Inhalte der Norm:

- Begriffe zum Thema Löschen
- Empfehlungen zur Dokumentenstruktur
- Verantwortlichkeiten
- Archiv und Backup
- Aussetzen von Löschung
- Organisation von Löschprojekten

Systemadministration und datenschutzgerechte Protokollierung systemübergreifend regeln lassen, ist dies auch für zentrale Aspekte der Löschung von Beschäftigtendaten möglich. In einer solchen »Grundlagenvereinbarung Löschen« könnten Grundsätze zur Löschung von Beschäftigtendaten vereinbart und Verfahren zur ordnungsgemäßen Entwicklung und Anwendung von Löschregeln festgeschrieben werden.

Vereinbart man in einer solchen Grundlagenvereinbarung die Anwendung der Norm DIN 66398, so ist sichergestellt, dass alle im Unternehmen verwendeten Datenarten mit einer Löschregel versehen sind. Es ist durchaus denkbar, dass die Belegschaftsvertretung bereits zum Projekt »Einführung Löschkonzept« mit dem Arbeitgeber verbindliche Beteiligungsformen vereinbart.

Zum Zeitpunkt der Erstverhandlung eines konkreten IKT-Systems müssten also die Datenflussanalyse abgeschlossen und die resultierenden Datenarten und Löschfristen bereits bekannt sein. Eine Übernahme der Löschregeln in Einzel-Betriebsvereinbarungen zu konkreten Systemen wäre demnach recht einfach. Diskussionen im Rahmen von Verhandlungen würden sich auf Fragen der Einordnung in Löschklassen, die resultierende Löschregel und auf Umsetzungsfragen konzentrieren – nicht aber, wie heute oft, auf die Frage, ob überhaupt gelöscht wird. Regelt die Einzelvereinbarung, wie üblich, präzise die Verwendungszwecke der Beschäftigtendaten, ergeben sich daraus die Datenarten und die resultierende Löschregel meist implizit.

Beides – Löschregel und Umsetzung – wären dann in einem Anhang der Einzelvereinbarung im gewünschten Detaillierungsgrad zu dokumentieren. Dabei hängt es sehr von den Spezifika des zu regelnden Systems ab, ob man sich mit der Benennung der Löschregel begnügen will oder auch konkrete Abläufe zur Umsetzung vereinbart.

Wie mit späteren Änderungen bezüglich Löschregeln umzugehen ist, sollte ebenfalls bereits in der skizzierten Grundlagenvereinbarung geregelt werden. »Einfache« Änderungen sollten möglichst ohne großen Aufwand durchgeführt werden können.

Die Beschäftigtenvertretung hat dabei auch die Aufgabe zu überprüfen, ob geschlossene Vereinbarungen eingehalten werden. Zu oft aber landet eine mit viel Energie verhandelte Vereinbarung nach der Unterschrift in den Schubladen beider Vertragspartner – und wird nur unvollkommen umgesetzt. Hier bietet die systematische Erstellung eines Löschkonzepts nach DIN 66398 zumindest Hilfestellung.

Löschmaßnahmen in Verfahren oder Systemen zur Verarbeitung von Beschäftigtendaten sollen nach der DIN 66398 über Umsetzungsvorgaben gesteuert werden. Diese dürfen sich nur innerhalb der Löschregeln aus dem Katalog bewegen. Anhand der Umsetzungsvorgaben kann der Betriebs- oder Personalrat prüfen, ob ein System kontinuierlich im Löschkonzept berücksichtigt wird. Außerdem kann er jederzeit konkrete Umsetzungsvorgaben daraufhin prüfen, ob dort alle Arten von Beschäftigtendaten im System vollständig aufgeführt und jeweils die vereinbarten Löschregeln zugeordnet und eingehalten werden.

Denn in den Umsetzungsvorgaben wird präzise beschrieben, was und wie gelöscht wird. Sie sind deshalb auch ein sehr guter Ausgangspunkt, um die Funktionstüchtigkeit der Löschmechanismen zu überprüfen. Es liegt deshalb nahe, dass in Regelprozessen des IKT-Betriebs solche Prüfungen regelmäßig durchgeführt werden, beispielsweise einmal im Jahr oder nach größeren Änderungen am System. Die Beschäftigtenvertretung sollte sich die Ergebnisse derartiger Überprüfungen regelmäßig zeigen und erläutern lassen.

Fazit

Mit Hilfe der Empfehlungen der DIN 66398 können Betriebs- und Personalräte ihre Unternehmen nicht nur zum datenschutzkonformen Löschen drängen, sondern auch zur Systematisierung und damit Vereinfachung üblicher Vereinbarungsdokumente beitragen. Wenn es gelingt, Löschregeln und Umsetzungsmaßnahmen für Beschäftigtendaten in der von der Norm empfohlenen Struktur festzulegen, wird eine einheitliche und handhabbare Löschdokumentation möglich. ◁

Dr. Volker Hammer, Secorvo Security Consulting GmbH, Karlsruhe
volker.hammer@secorvo.de

Karin Schuler, Secorvo Security Consulting GmbH, Karlsruhe;
karin.schuler@secorvo.de
auch: Datenschutz & IT-Sicherheit, Bonn; **buero@schuler-ds.de**