KERSTIN BLOSSEY,
BLOSSEY & PARTNER

Heißer Herbst für den deutschen Datenschutz 2009

Praxisrelevante Aspekte der aktuellen Änderungen des BDSG

Schwierigkeitsgrad:

Durch die Skandale von Behörden und der freien Wirtschaft, die in der Weltpresse ihre Runden gezogen haben, hat sich ein politischer Druck aufgebaut, der 2009 endlich so hoch kochte, dass die Volksvertreter den seit Jahren von Fachverbänden und Datenschutzexperten geforderten Änderungen der Gesetzeslage Raum gegeben haben, statt diese Aufgabe in die nächste Legislaturperiode zu schieben, wie es allzu häufig zu beobachten war. Doch die Änderungen werden nicht von allen Fachleuten, die in der Datenschutzpraxis zu hause sind, als brauchbare Verbesserungen zum Schutz der Privatsphäre im Zeitalter globaler Informationszentralisierung interpretiert.

IN DIESEM ARTIKEL ERFAHREN SIE...

Was sich durch die Neufassung des BDSG ändert;

Wann die neuen Regelungen in Kraft treten;

Welche Aspekte für die Praxis besonders wichtig werden;

WAS SIE VORHER WISSEN/ KÖNNEN SOLLTEN...

Keine spezifischen Vorkenntnisse erforderlich, die Grundbegriffe des Datenschutzes aus den Artikeln der vorherigen Ausgaben sollten geläufig sein. Alternativ kann auf das Glossar von Blossey & Partner (*http://blossey-partner.de/showpage.php?SiteID=11&lang=1*) zurückgegriffen werden.

Novellierung des BDSG in drei Akten

Die umfassende Neugestaltung des Bund esdatenschutzgesetzes (BDSG) wurde in den letzten Jahren immer wieder diskutiert, doch insbesondere die zeitgemäßere Orientierung bei so manchen Punkten wurde immer wieder gescheut. Nach der letzten Änderung durch das „Erste Gesetz zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft" 2006 finden sich mit den drei Novellen von 2009 gleich zwei grundlegende Reformen: zum einen das Thema „Scoring" inkl. der Tätigkeiten von Auskunfteien, zum anderen die generelle „Verschärfung" des betrieblichen Datenschutzes im öffentlichen und nicht-öffentlichen Bereich. Am 10.07.2009 stimmte der Bundesrat der Novellierung des BDSG zu, in dem er das „Gesetz zur Änderung datenschutzrechtlicher Vorschriften" beschloss. Er ebnete damit den Weg zu einer dreistufigen Änderung der nationalen Umsetzung der EU-Richtlinie 95/46.

Die folgende Tabelle zeigt die Novellen I – III zum BDSG im Überblick.

Die Übergangsfristen hierzu sind in § 47 BDSG der neuen - zum Zeitpunkt des Verfassens dieses Artikels nichtamtlichen - Fassung geregelt: „Für die Verarbeitung und Nutzung vor dem 1. September 2009 erhobener oder gespeicherter Daten ist § 28 in der bis dahin geltenden Fassung weiter anzuwenden:

- für Zwecke der Markt- oder Meinungsforschung bis zum 31. August 2010,
- für Zwecke der Werbung bis zum 31. August 2012"

Weitere Details zu den Novellen können der entsprechenden Synopse entnommen werden.

Aktuelle Kernpunkte der Novellen

Wie aus der Datierung der Novellen zu erkennen ist, beschäftigt derzeit vor allem Novelle II die Fachleute, die bereits zum 1. September

diesen Jahres in Kraft treten wird. Das Gesetzgebungsvorhaben zum Datenschutzauditgesetz (DSAG) wurde auf Grund des allzu komplexen Verfahrens gestrichen, es ist aber ein dreijähriges Pilotprojekt für eine Branche vorgesehen. Sehen wir uns im Folgenden daher einige Änderungen an, die sich unmittelbar auf die Praxis auswirken werden – mit dem Fokus auf die Novelle II.

Werbung, Datenübermittlung, Listenprivileg und die Einwilligung

Wie schon immer gilt auch weiterhin die Einwilligung des Betroffenen in die Verarbeitung seiner personenbezogenen Daten als optimaler Weg zur Nutzung seiner Daten. Erfolgt diese Zustimmung des Betroffenen in Zusammenfassung mit weiteren Erklärungen, die abgegeben werden sollen, ist nun ausdrücklich dafür zu sorgen, dass der Text zur Einwilligung der Datenverarbeitung „in drucktechnisch deutlicher Gestaltung besonders hervorgehoben" werden muss. Erfolgt die Einwilligung nicht schriftlich, ist sie durch die verantwortliche Stelle schriftlich zu bestätigen. Der Bundesgerichtshof hat mit Urteil vom 16.07.2008 allerdings betont, dass ein solches Vorgehen nicht für die werbliche Ansprache per Telefon, SMS, Fax oder E-Mail. Hier ist die ausdrückliche Einwilligung (Opt-In) Voraussetzung.

Eine Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung ist grundsätzlich nur mit Einwilligung der Betroffenen möglich. Das Listenprivileg des § 28 Absatz 3 Satz 1 Nummer 3 BDSG (bisherige Fassung) wird zum Listendatenprivileg nach dem neuen § 28 Absatz 3 BDSG modifiziert. Es ermöglicht fünf Ausnahmen vom Einwilligungserfordernis, wenn allein nicht-sensible Listendaten für Werbezwecke verarbeitet und genutzt werden. Folgenden Merkmale sind hier erlaubt:

- Personengruppen-Zugehörigkeit (als gemeinsames Listenmerkmal),
- Berufs-, Branchen- oder Geschäftsbezeichnung,
- Name,
- Titel und akademischer Grad,
- Anschrift,
- Geburtsjahr.

Weitere Daten wie etwa E-Mail-Adresse, Rufnummer oder vollständiges Geburtsdatum fallen nicht hierunter.

Das neue Listendatenprivileg findet seine Anwendung in folgenden – thematisch zusammengefassten – Bereichen:

- **Eigenwerbung**
  Zulässig, wenn die Daten direkt beim Betroffenen im Rahmen eines Vertragsverhältnisses (oder eines vertragsähnlichen Verhältnisses) bzw. aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren Verzeichnissen erhoben wurden. Wichtig: Das Internet als solches ist nicht als Verzeichnis zu verstehen, entsprechend aus dem Scannen online verfügbarer Veröffentlichungen gewonnene Daten sind nicht als rechtmäßig erhoben zu verstehen.
  Nach § 28 Abs. 3 Satz 3 BDSG darf die verantwortliche Stelle diese Daten zu eigenen Zwecken anreichern, wenn diese ebenfalls rechtmäßig zu einem anderen Zweck erhoben oder übermittelt worden sind, beispielsweise zur Verbesserung der Kunden- oder Vertragsbeziehung im Rahmen des § 4 Absatz 3 BDSG. Längst gängige Praxis ist hiermit legitimiert.
- **Fremdwerbung**
  Die Nutzung eigener Daten zum Zweck der Werbung für fremde Angebote – insbesondere beim so genannten „Empfehlungsmarketing" - ist zulässig. Jedoch muss die verantwortliche Stelle klar erkennbar sein – das bedeutet, dass generell die Stelle, die den betroffenen Datensatz erhoben hat, genannt werden muss, selbst wenn durch die Übermittlung der Informationen mehrere Stellen dazwischen stehen können. Hier wäre beispielsweise ein Hinweissatz praktikabel. In der Praxis bedeutet dies sicherlich mehr Transparenz für den Betroffenen im Falle von Lieferketten und damit die Möglichkeit für eine bessere Einflussname in Bezug auf Werbewiderspruch und Auskunftsersuchen. Für die verantwortliche Stelle kann dies aber auch die Brandmarkung zum „Datenverkäufer" bedeuten. Die Aufbewahrungsfrist von zwei Jahren im Bereich des Listendatenprivilegs (§ 34 Absatz 1a BDSG) soll die Betroffenenrechte sichern.
- **Business-to-Business (b2b)**
  Weiterhin zulässig, sofern beachtet wird, dass freiberuflich oder gewerblich Tätige ausschließlich auf ihrer geschäftlichen Basis und ausschließlich für beruflich bedingten Bedarf angesprochen werden. Das Vorhandensein einer privaten Wohnung an derselben Adresse schadet dagegen nicht.
- **Spenden**
  Zulässig unter der Voraussetzung, dass die Zuwendungen nach §§ 10b und 34 Einkommensteuergesetz (EStG) steuerbegünstigt sind.

Für den Markt- und Meinungsforschungsbereich gilt ab sofort eine eigenständige Norm, nämlich § 30a BDSG. Besonderheit für diese Branche ist wohl vor allem die generelle Pflicht zur Bestellung eines DSB nach § 4f Absatz 1 Satz 4 BDSG. Der Bereich Scoring und Auskunfteien wird ab Herbst durch eigenständige Regelungen in § 28b BDSG behandelt.

Wochenrückblick zu den Datenschutz-Schlagzeilen in der Online-Presse:

Das Redaktionsteam von Blossey & Partner stellt jede Woche neu die Schwerpunktthemen rund um Datenschutz für Sie zusammen unter http://www.blossey-partner.de („News", unten rechts). Gucken Sie doch mal rein, das Archiv reicht inzwischen bis 2005 zurück und bietet sogar eine Suchfunktion. Viel Spaß beim Stöbern.

Stärkung des DSB und der Aufsichtsbehörden

Der betriebliche Datenschutzbeauftragte (DSB) erhält nach § 4f Absatz 3 Satz 4f BDSG einen verbesserten Kündigungsschutz, der eine ordentliche Kündigung innerhalb eines Jahres nach seiner Abberufung als DSB verbietet, sofern die Kündigung nicht „aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist" erfolgt. Voraussetzung hierfür ist die Erforderlichkeit zu einer Bestellung.

Der DSB wird in dieser Frage quasi dem Betriebsrat gleichgestellt, auch insoweit, dass er zur „Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde" ein Recht auf die kostenfreie „Teilnahme an Fort- und Weiterbildungsveranstaltungen" zu Lasten der verantwortlichen Stelle. Insoweit könnte die Abwägung zwischen intern und extern bestelltem DSB verstärkt in Richtung externem Dienstleister gehen, da dieser in der Regel einfach nach den vertraglich vereinbarten Regeln kündbar ist und die Fachkunde samt ständiger Updates durch die Einbindung in ein Fachgremium hier Grundvoraussetzung sind.

Die Weisungsbefugnis der Aufsichtsbehörden wird erweitert. Auf diese Weise drohen damit nicht nur Bußgelder, sondern zusätzlich unmittelbare Anordnungen und gegebenenfalls - statt bisher nur die Untersagung einzelner Verfahren, sogar umfassende Untersagungen in Bezug auf materiell rechtswidrige Datenverarbeitungen nach § 38 Absatz 5 Satz 2 BDSG.

Der Bußgeldrahmen nach § 43 BDSG wurde ebenfalls erhöht: bis zu 50.000 € für Verstöße gegen Verfahrensvorschriften, bis zu 300.000 € bei Verstößen gegen materielle Schutzvorschriften. Die „Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat", allerdings „übersteigen", so dass die Höchstbeträge nur markiert, nicht gesetzt, sind.

Zusammenarbeit mit externen Anbietern (Outsourcing)

Die Verlagerung von Aufgaben eines Unternehmens an einen externen Partner ist bereits nach herkömmlichem BDSG recht konkret formuliert. So ist der Auftragsnehmer nicht nur sorgfältig nach den Datenschutzanforderungen auszuwählen, sondern er ist gegebenenfalls auch durch den Auftraggeber zu überprüfen, um als verantwortliche Stelle die Kontrolle über die ihm anvertrauten personenbezogenen Daten behalten zu können. Die Novelle II bringt hier keine wesentlichen Neuerung, verschärft jedoch die bereits bestehenden Anforderungen. Vor allem wird sich die nun umfassende Dokumentations- und Kontrollpflicht durch den Auftraggeber in der Praxis auswirken. Aufträge sind ab 01.09.2009 in jedem Fall schriftlich zu erteilen und müssen ab dann zumindest die folgenden Aspekte regeln:

- Gegenstand und Dauer des Auftrags,
- Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
- die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
- die Berichtigung, Löschung und Sperrung von Daten,
- die nach Absatz 4 bestehenden Pflichten des Auftragsnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
- die etwaige Berechtigung zur Begründung von Unterauftragsverhältn issen,
- die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragsnehmers,
- mitzuteilende Verstöße des Auftragsnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
- der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragsnehmer vorbehält
- die Rückgabe überlassener, Datenträger und die Löschung beim Auftragsnehmer gespeicherter Daten nach Beendigung des Auftrags.

Die Einhaltung der Datenschutzanforderungen muss der Auftraggeber künftig in regelmäßigen Abständen kontrollieren und die Ergebnisse dieser Überprüfung zudem schriftlich festhalten. Zuwiderhandlungen fallen ab Herbst nach § 43 Absatz 1 Nummer 2b. BDSG unter die Ordnungswidrigkeiten und können mit bis zu 50.000 Euro geahndet werden.

Pflicht zur Auskunft und Information über Datenschutzpannen

Die Betroffenenrechte werden gestärkt, und zwar sowohl in Form konkretisierter Aufbewahrungsfrist und Benennung der tatsächlichen Daten-Empfänger als auch in Form der Auskunft auch über Daten, die nicht automatisiert verwendet sind. Diese Regelungen sind jeweils auf bestimmte Anwendungsbereiche zugeschnitten, so dass sich hier die Lektüre des § 34 BDSG empfiehlt.

Der neu geschaffene § 42a BDSG führt die „Informationspflicht bei

Novelle I (tritt in Kraft am 01.04.2010)	Novelle II (01.09.2009)	Novelle III (11.06.2010)
Konkretisierung Scoring	Personalisierte Werbung	Umsetzung der Verbraucherkreditrichtlinie
Automatisierte Einzelentscheidungen	Verschärfte Anforderungen an die Auftragsdatenverar beitung	
Datenübermittlung an Auskunfteien	Arbeitnehmerdatenschutz	
	Informationspflicht über Datenpannen	
	Kündigungsschutz für den DSB	

unrechtmäßiger Kenntniserlangung von Daten“ ein und soll auf diese Weise einerseits das Prinzip der Selbstkontrolle stärken, andererseits für mehr Transparenz bei Betroffenen, Aufsichtsbehörden und gegenüber der Öffentlichkeit sorgen. Die Offenlegung solcher Datenschutzpannen sieht jedoch zugleich ein paar Ausnahmen und Einschränkungen vor, die wieder als Hintertürchen gewertet werden und folglich dazu führen könnten, dass diese Vorschrift wenig ernst genommen wird. So ist beispielsweise eine Information über ein solches Vorkommnis – sofern „die Information der Betroffenen ansonsten einen unverhältnismäßigen Aufwand erfordern würde“ – in „mindestens zwei bundesweit erscheinenden Tageszeitungen“ vorgesehen, jedoch können auch andere „in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete“ Maßnahmen getroffen werden.

Beschäftigtendatenschutz

Der Begriff „Beschäftigtendatenschutz“ ersetzt künftig den bisher geläufigen „Ar beitnehmerdatenschutz“. Die geänderte Bezeichnung soll die Betroffenengruppe konkretisieren, da nach Datenschutz nicht nur klassische Vollzeitangestellte, sondern beispielsweise auch Teilzeit- und Honorarkräfte, „Minijobler“, Praktikanten, Auszubildende, Wehrdienst- und Wehrersatzdienstleistende oder auch ehrenamtliche Kräfte hierunter zu zählen sind. Auch die personenbezogenen Daten von Bewerbern sind zu berücksichtigen. Der genaue Wortlaut kann hierzu § 3 Absatz 11 BDSG entnommen werden.

Wer erwartet, dass statt dem ursprünglich und seit vielen Jahren geforderten Arbeitnehmerdatensch utzgesetz nun wenigstens im neuen BDSG eine annähernd angemessene Regelung zu den wichtigsten Eckdaten der Beschäftigten ihren Einzug genommen hat, muss sich von dieser Wunschvorstellung verabschieden. Zwar gibt der neu geschaffene § 32 BDSG einen Hinweis darauf, dass es einen Beschäftigtendatenschutz in irgendeiner Form geben mag, geregelt wird im novellierten BDSG hingegen wenig zu konkreten Anforderungen zum Schutz der Arbeitnehmer am Arbeitsplatz.

Im Wesentlichen scheint der Gesetzgeber mit diesem Paragraphen vor allem den Skandalen um Mitar beiterdaten begegnet sein zu wollen, dürfen doch ab Herbst nur dann personenbezogene Personaldaten zur Aufdeckung von Straftaten verwen det werden, wenn tatsächliche Verda chtsmomente und Anhaltspunkte den Verdacht auf strafbares Handeln untermauern.

Fazit: Ein heißer Datenschutz-Herbst – und es bleibt spannend!

Neben den Diskussionen diverser Interessengruppen und den durchaus berechtigten Vorbehalten gegen die eine

oder andere Formulierung beschäftigt die Datenschutzfachleute vor allem die Frage, welche Auswirkungen sich auf die unternehmerische Praxis tatsächlich ergeben werden. Derzeit ist keineswegs klar, welche Erwartungen die Regierung im Einzelnen an die Aufsichtsbehörden haben – und daher ist es derzeit völlig ungewiss, wie die Aufsichtsbehörden ihre neuen Kompetenzen verstehen und leben werden.

Praktisch gesehen ist eine detaillierte Vertragsgestaltung mit externen Geschäftspartnern, Dienstleistern und Anbietern sicherlich eine Aufgabe, die jede verantwortliche Stelle im eigenen unternehmerischen Interesse ab sofort besonders sorgfältig erledigen sollte. Wer seine „Hausaufgabe" in Form von Vertragsanlagen für bereits bestehende Verträge und eine entsprechende Konkretisierung für Neuverträge schon gemacht hat, wird sich ab Herbst in einem klaren Vorteil befinden.

Wer noch keinen DSB bestellt hat, entweder aus Fragen der Priorität des Themas oder weil bisher nicht zwingend vorgeschrieben, wird genauer abwägen müssen, ob in Anbetracht des erweiterten Kündigungsschutzes eines internen DSB die externe Lösung die wirtschaftlichere und unternehmensfreundlicher Alternative sein könnte.

Wer bisher ein Freund der werblichen Ansprache war und hier stillschweigend auf fragwürdige Datenstämme zurückgegriffen hat, muss sich dies ab 01.09.2009 genauer überlegen, da hier durch eine erfahrbare Steigerung der Sensibilität der Verbraucher, der Medien und der Öffentlichkeit neben Bußgeldverfahren, Audits durch die zuständigen Aufsichtsbehörden vor allem ein massiver Imageschaden droht, der bisher oftmals völlig unterschätzt wird. Zusätzlich ist mit verstärkten Kontrollen der Behörden zu rechnen, zumal einige Dienststellen aufgestockt wurden. Beispielsweise wurde in Bayern der für den Datenschutz im nicht-öffentlichen Bereich (z. B. Privatwirtschaft) der Regierung von Mittelfranken nicht nur personell massiv erweitert, hier wurde sogar eine eigenständige Einheit in Form des „Landesamt für Datenschutzaufsicht" geschaffen. Also ist von pfiffigen Unternehmern nun auch der politische Druck auf die Behörden, Ergebnisse zu präsentieren, mit zu berücksichtigen bei der Abwägung des „einkalkulierten Risikos" - sofern man nicht gewillt ist, Datenschutz als Qualitätsmerkmal und geltendes Gesetz zu akzeptieren.

Bisher war „nur" die Erhebung oder Verarbeitung sanktioniert, ab Herbst 2009 wird nun auch die Nutzung rechtswidrig erhobener personenbezogener Daten eine Ordnungswidrigkeit darstellen. Bislang konnte der Adresshändler im Zweifelsfall die Verantwortung stets auf die Drittfirma verlagern, die die Adressdaten erhoben hatte. Zudem sind Adresshändler künftig verpflichtet, bei automatisierten Abrufverfahren stichprobenartig das tatsächlich berechtigte Interesse des Dritten zu überprüfen.

Unabhängig davon besteht natürlich wie bisher für jede Personendaten verarbeitende Stelle die Anforderung einer dem Unternehmen angemessenen Datenschutzorganisation. Neben der Mitarbeitersensibilisierung („Was ist Datenschutz und was habe ich diesbezüglich bei meiner Arbeit zu beachten?") zählen vor allem die unter Datenschutz-Fachleuten gerne „TOMs" genannten technischen und organisatorischen Maßnahmen, wie sie § 9 BDSG und Anlage zum § 9 BDSG vorschreiben. Hier zeigen immer noch vielfach Studien und andere Untersuchungsergebnisse, dass Unternehmen das Thema Sicherheit generell zu niedrig bewerten. Die Folge sind ungeschützte PC-Arbeitsplätze, nur grob zerrissene Papierdokumente mit teils überaus sensiblen und personenbezogenen Informationen, auf dem Firmengelände umher irrende Besucher und die oft viel zu sorglose Weitergabe personenbezogener und unternehmenssensibler Daten an unbekannte Dritte. Solange hier kein massives Umdenken - von Betroffenen und verantwortlichen Stellen gleichermaßen! - stattfindet, werden weiterhin Informationen, die eigentlich in die Privatsphäre des jeweils Betroffenen gehören sollten, auf Datenträgern verkauft werden, Kundendatenbanken entwendet und gehandelt werden, innovative Ideen und Produkte durch Dritte realisiert, bevor man selbst dazu gekommen ist.

Als *Datenschutzberaterin* und externe Datenschutzbeauftragte finde ich es erschreckend, welchen Zulauf soziale Plattformen im Internet haben; insbesondere wenn man beobachtet, wie viele wirklich private Informationen der User über sich selbst und zu allem Unglück auch noch über andere, die hiervon teilweise gar nichts ahnen, preisgibt. Es ist längst kein Geheimnis mehr, dass Unternehmen ebenso wie Behörden das Internet aktiv nutzen, sobald ein neuer Kontakt ins Spiel kommt. Man sucht nach allem, was den fremden Ansprechpartner transparenter macht und bildet sich ein erstes „Vor-Urteil" über die Person, bevor man sie kennen gelernt hat. Als *Unternehmerin* begrüße ich hingegen die Vielzahl vollkommen „unschuldiger" Datenquellen im WordWideWeb natürlich, denn auch mir eröffnen sich dadurch oft völlig neue Perspektiven, etwa wenn es um ein Bewerbergespräch oder das Aushandeln von Konditionen geht. Als *Betroffene* wäre mir allerdings die „informationelle Chancengleichheit", gerade als Mensch gegenüber einem mir erst einmal anonym bekannt gewordenen Unternehmen, mit dem ich etwas Gemeinsames vereinbaren möchte, vielfach lieber. Bleibt also nur zu hoffen, dass möglichst wenige Menschen über mich online persönliche Informationen verbreiten, ohne dass ich davon weiß. Vielleicht kann das BDSG dazu beitragen – aber der Löwenanteil wird weiterhin von der Selbstkontrolle jedes Betroffenen und der verantwortlichen Stellen abhängen.

Zur Autorin

Kerstin Blossey ist Dipl. Informations-Wirtin (FH) und Gründerin von Blossey & Partner, einer aufstrebenden Unternehmensberatung, die sich ganz auf den unternehmerischen Datenschutz spezialisiert hat. Zum Kundenkreis zählen deutsche wie international angesiedelte mittelständische Unternehmen, Konzerne und Einrichtungen aus so unterschiedlichen Branchen wie Druck & Medien, Telekommunikation, Verlagswesen, Softwareindustrie, Automotive, Wirtschaft, Gesundheitswesen, Tourismus und der öffentlichen Hand. In gelegentlichen Fachbeiträgen und Vorträgen vermittelt sie schwerpunktmäßig Möglichkeiten und Wege des praxisorientierten Datenschutzes.