BDSG-Novelle 2009: Umsetzung der ADV

GDD-Erfa-Kreis-Sitzung Sommerworkshop

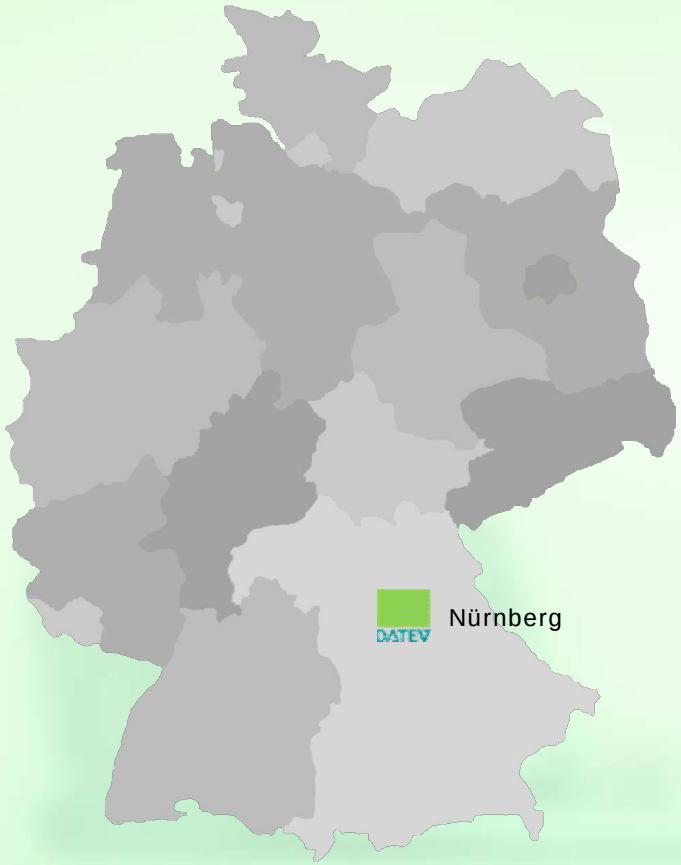
Stuttgart, 8. Juni 2011

Beate Beißwenger,
Datenschutzreferentin, DATEV eG

Themen

1. DATEV eG
2. Datenschutzmanagement
3. Umsetzung der BDSG Novelle
4. Überprüfungspflicht / Audit

Das Unternehmen



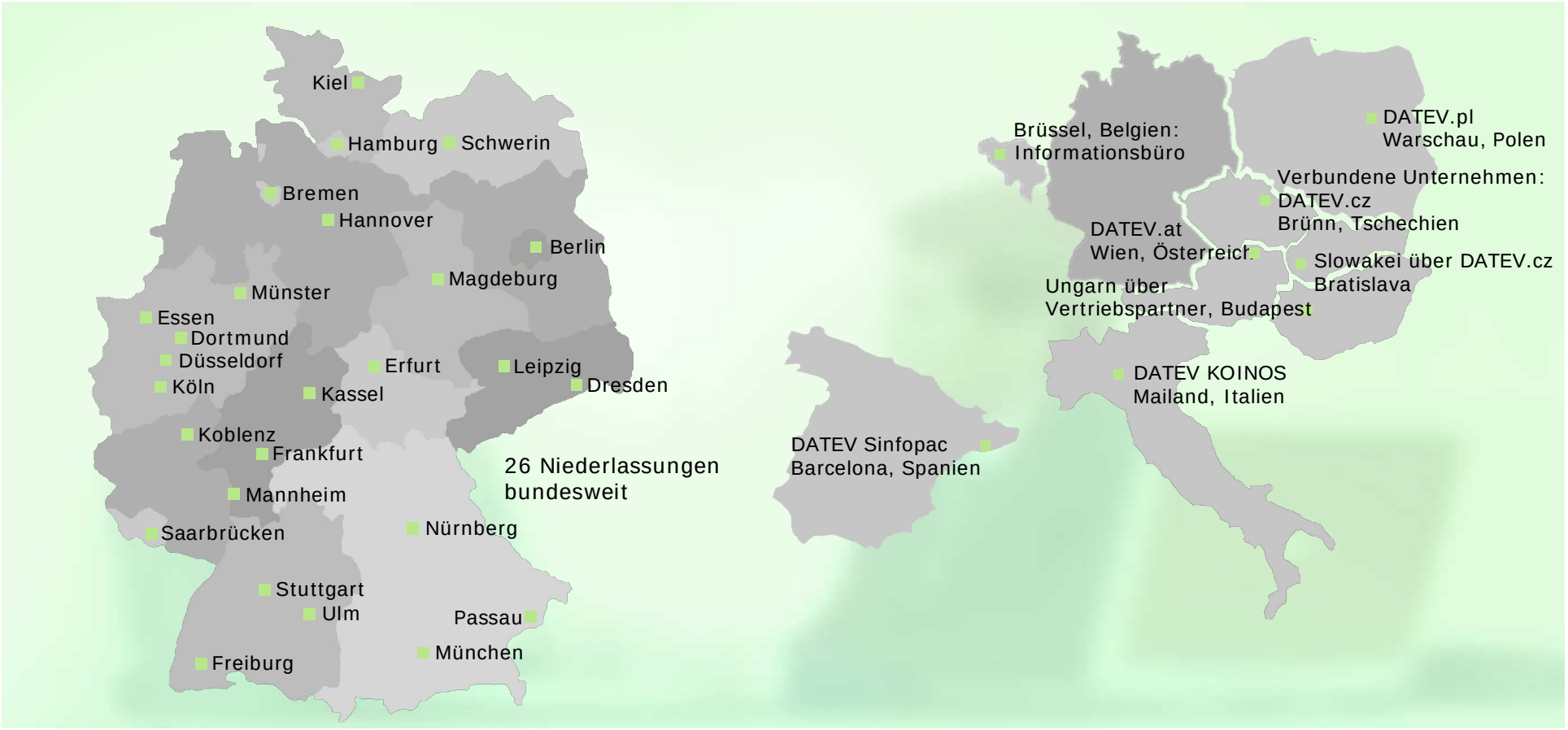
DATEV eG
Hauptsitz: Nürnberg
Gründung: 1966

Berufsständische EDV-Dienstleistungsorganisation in Europa für

- Steuerberater
- Rechtsanwälte
- vereidigte Buchprüfer
- Wirtschaftsprüfer

Das Unternehmen

Niederlassungen, Informationsbüros in Berlin und Brüssel sowie verbundene Unternehmen



DATEV: Auftrag und Mitglieder

Unser Auftrag

- Wirtschaftliche Förderung unserer Mitglieder (39.756 in 2010)
- Das bedeutet: Unterstützung bei allen Dienstleistungen unserer Mitglieder für deren Mandanten

Unsere Mitglieder

- Steuerberater
- Rechtsanwälte
- Wirtschaftsprüfer
- Vereidigte Buchprüfer
- Sozietäten und Partnergesellschaften
- Gesellschaften der Berufsangehörigen

DATEV – Mitglied – Mandant

DATEV-Kunden: Mitglieder und deren Mandanten

Leistungsspektrum

Software
z. B.

- Rechnungswesen
- Abschlussprüfung
- Personalwirtschaft
- Wirtschaftsberatung
- Kanzleiorganisation

2,5 Mio. Finanzbuchführungen über 10 Mio. Lohnabrechnungen pro Monat

Service
z. B.

- persönlicher Service
- Anwendungen
- IT Support
- Druck- und Versandservice

ca. 1000 Mitarbeiter leisten ca. 2,4 Mio. Servicekontakte im Jahr 2010

Beratung / Wissen
z. B.

- Consulting
- Training
- Weiterbildung
- Fachliteratur
- Datenbanken

ca. 82.000 Teilnehmer an DATEV-Seminaren

Themen

1. DATEV eG
2. Datenschutzmanagement
3. Umsetzung der BDSG Novelle
4. Überprüfungspflicht/Audit

Umsetzung BDSG Novelle

Verhaltenskodex

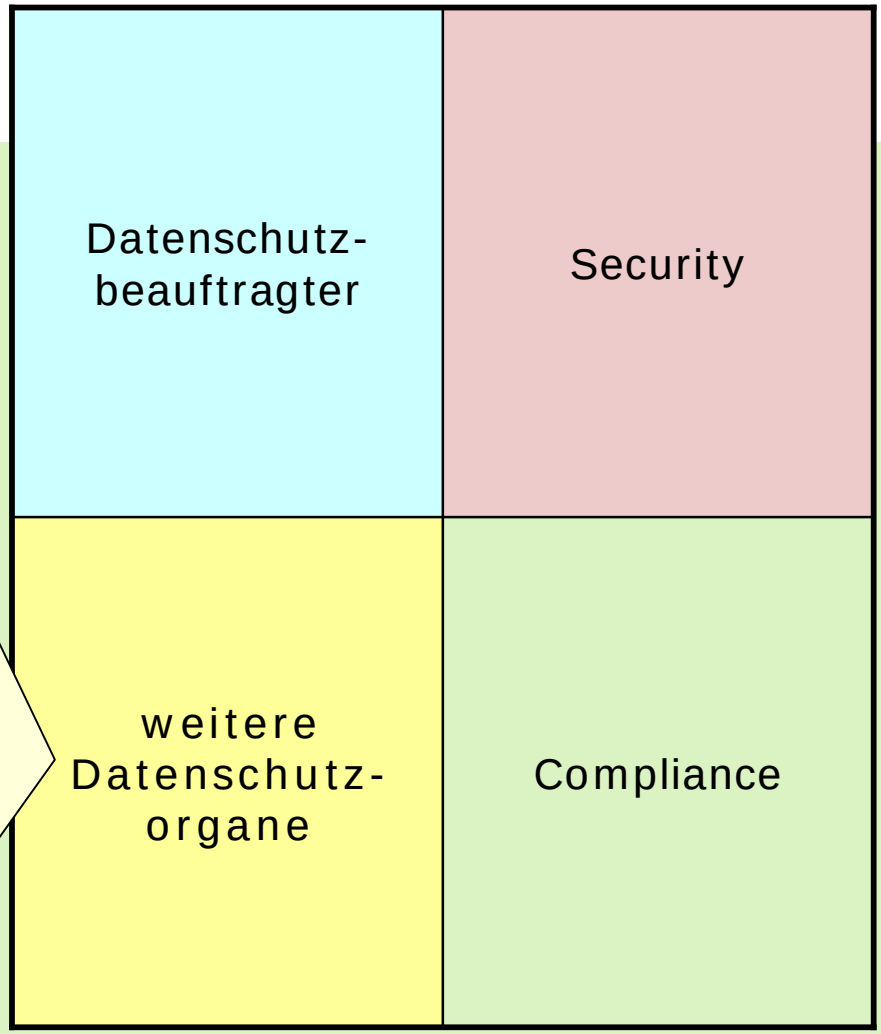
Art. 2 Datenschutz und Datensicherheit

Für DATEV als berufsständischen DV-Dienstleister haben Datensicherheit und Datenschutz oberste Priorität und sind von grundlegender Bedeutung.

DATEV steht für außergewöhnlich hohe Standards in diesem Bereich. Dies gilt in besonderer Weise für personenbezogene Daten, aber auch für Geschäftsdaten. Allen Mitarbeitern obliegt in diesem Zusammenhang eine besondere Verantwortung.	Alle Mitarbeiter wahren die strikte Vertraulichkeit von Mitglieds- und Mandantendaten, insbesondere von Auftragsdaten.	DATEV verlangt von allen Geschäftspartnern die Einhaltung der Verpflichtungen zum Datenschutz und zur Datensicherheit sowie zur Wahrung der Vertraulichkeit.

Datenschutzorganisation: intensive Vernetzung

- Datenschutzausschuss
- Bereichsbeauftragte für den Datenschutz
- Sicherheit/Betriebsschutz
- Sicherheitsingenieur
- IT-Sicherheit
- Revision
- Rechtsabteilung
- DATEV-DSB (Consulting)



Themen

1. DATEV eG
2. Datenschutzmanagement
3. Umsetzung der BDSG Novelle
4. Überprüfungspflicht/Audit

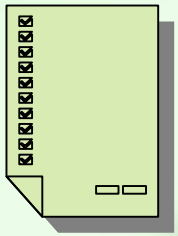
Umsetzung BDSG Novelle

Zeitplan

- Beschluss des Bundestags am 3. Juli 2009
- Zustimmung des Bundesrats am 10. Juli 2009
- Ausfertigung im Bundesgesetzblatt am 14. August 2009
- Geltung der BDSG-Novelle II ab 1. September 2009

Konsequenz der Gesetzesänderung

Schwerpunkte



Auftragsdaten-
verarbeitung

Beschäftigten-
datenschutz

Verschlüsselung

Datenpanne

Listenprivileg
(Adresshandel)

Kommunikations-
konzept

Konsequenz der Gesetzesänderung

Vorgehensweise

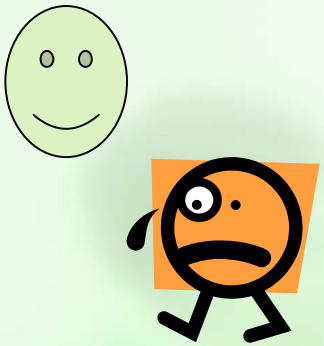
Beschäftigten-Datenschutz:	kein unmittelbarer Handlungsbedarf
Listenprivileg (Adresshandel):	kein unmittelbarer Handlungsbedarf
Verschlüsselung:	DATEV-Security-Lösungen / Datenschutzkontrolle
Datenpanne:	eigener Prozess erforderlich
Auftragsdaten-verarbeitung:	als Auftraggeber und Auftragnehmer
Kommunikations-Konzept:	Einbindung weiterer Stellen

Auftragsdatenverarbeitung

Was hat sich geändert?

- Die schriftliche Beauftragung hat nun Pflichtinhalte, die in § 11 Abs. 2 BDSG aufgezählt sind.
- Der Auftraggeber muss sich vor Beginn der Datenverarbeitung und dann regelmäßig vom Datenschutzniveau des Auftragnehmers überzeugen.
- Sowohl Einhaltung der schriftlichen Beauftragung als auch Kontrolle vor Beginn der DV sind bußgeldbewehrt (50.000 €).

Auftragsdatenverarbeitung



Konsequenzen als Auftraggeber

Datenschutz ist als Auswahlkriterium gestärkt worden

Alle Lieferantenverträge prüfen, ergänzen, Datenschutz kontrollieren

Besonderheit: A-DV auch bei Wartung (§ 11 Abs. 5 BDSG):

„wenn Prüfung oder Wartung ... im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann."

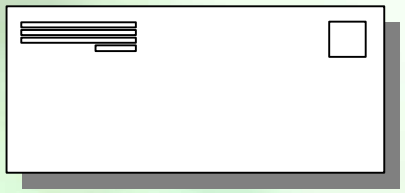
Beispiele: Server, PCs, Fax, Fernwartung

Auftragsdatenverarbeitung

Konsequenzen als Auftraggeber:

- ✓ Information und Schulung des Einkaufs
- ✓ Checkliste für Einkäufer
- ✓ Prozessinitialisierung und unterstützen
  ➔ Prüfung der TOMs durch IT-Sicherheit
- ✓ Prüfungsumfang der TOMs abhängig von Vertraulichkeitsklasse
- ✓ Alle Lieferantenverträge prüfen, ergänzen, Datenschutz kontrollieren

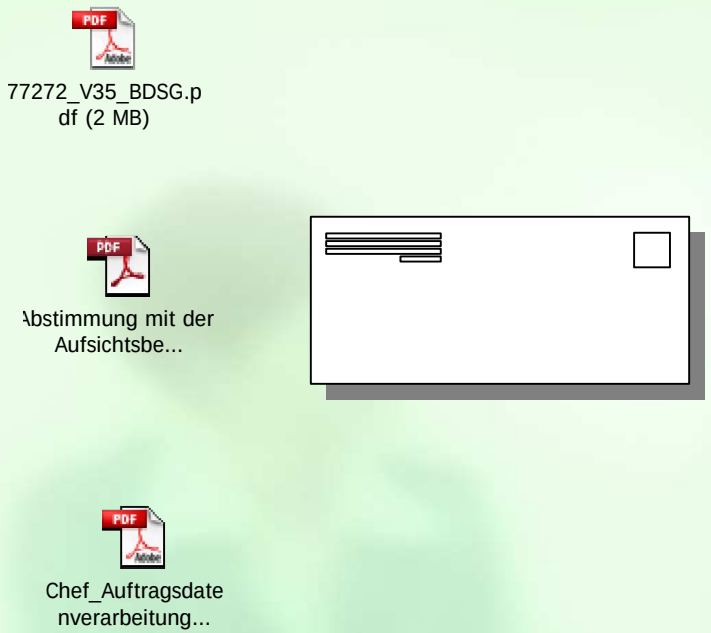
Auftragsdatenverarbeitung



Konsequenzen als Auftragnehmer:

- ✓ Vertragsergänzungen mit allen Kunden
- ✓ individuelle Anschreiben mit Vertragsangebot
- ✓ zusätzliche Informationen in DATEV-Magazin, Trialog, Podcast

Auftragsdatenverarbeitung



Konsequenzen als Auftragnehmer

- ✓ Information der Mitglieder über Änderungen im September 2009
- ✓ Abstimmung mit der Aufsichtsbehörde Anfang Dezember
- ✓ individuelle Anschreiben mit Vertragsangebot im Dezember 2009 mit Hotline-Angebot

Auftragsdatenverarbeitung

Gestaltung der Auftragsdatenverarbeitung:

- ✓ Vorlage BITKOM-Entwurf von Ende November 2009
- ✓ als Rahmenvereinbarung in Ergänzung der Beitrittserklärung und den AGBs
- ✓ individuelle Angaben (Art/Umfang, Betroffene) über Auftrag/ Leistungsbeschreibung
- ✓ „Schriftform" über § 151 Satz 1 BGB gelöst
- ✓ allgemeine Fassung der TOMs mit Bayerischer Aufsichtsbehörde abgestimmt

Auftragsdatenverarbeitung

Kennzahlen der Umsetzung als Auftragnehmer:

- ✓ angeschrieben ca. 64.000 Kunden im Dezember 2009/Februar 2010
- ✓ Erinnerungsaktion im April/Mai 2010
- ✓ über 1,35 Mio. Druckseiten
- ✓ ca. 94.000 Sendungen
- ✓ 3 Aushilfen in Posteingang
- ✓ ca. 2.200 Anrufe bei der Hotline

Themen

1. DATEV eG
2. Datenschutzmanagement
3. Umsetzung der BDSG Novelle
4. Überprüfungspflicht / Audit

Kontrolle des Auftragnehmers

§ 11 (2) BDSG

Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

Das Ergebnis ist zu dokumentieren.

wie?

- Selbstauskünfte des Auftragnehmers, z. B. dessen TOMs
- Testat eines Sachverständigen
- persönlich vor Ort

Kontrolle des Auftragnehmers

§ 9 a BDSG

Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungs-systemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

- nach 10 Jahren immer noch kein Bundesgesetz zum Datenschutzaudit

Hintergrundinformationen zum Datenschutz-Audit nach § 9a

Im Fokus steht die Überprüfung des Datenschutz-Management-systems durch einen unabhängigen und zugelassenen Gutachter.

Auf dem Prüfstand steht die gesamte Datenschutz-Organisation.

Alle unternehmensinternen Regelungen, Mechanismen und Prozesse, die einen gesetzeskonformen Umgang mit personenbezogenen Daten und insbesondere die datenschutzgerechte Datenverarbeitung sicherstellen sollen.

Auswahl des Zertifiziers: DQS

- DQS: Deutsche Gesellschaft zur Zertifizierung von Manangementsystemen
- seit 1985 Zertifizierer von Managementsystemen
- zugelassen für die Zertifizierung von mehr als 100 national und international anerkannten Normen
- einer der Marktführer mit Begutachtung von jährlich rund 47.000 Managementsystemen
- 374 Zertifizierungen nach ISO 27001

Quelle: DQS

BDSG-Themen des Datenschutz-Audits (Auszug)

Besondere Formen des Umgangs mit personenbezogenen Daten

§ 6b	Beobachtung öffentlicher Räume mit Video
§ 6c	Mobile personenbezogene Speicher-/Verarbeitungsmedien
§ 9a	Datenschutz-Audit

Zulässigkeit/Rechtsgrundlage

§ 3a	Datenvermeidung/-sparsamkeit
§ 4	Zulässigkeit Datenerhebung, -verarbeitung, -nutzung
§ 28	Datenerhebung/-verarbeitung für eigene Zwecke
§ 32	Datenerhebung, -verarbeitung für Zwecke des Beschäftigungs-verhältnisses
§ 4a	Einwilligung

Rechte des Betroffenen

§ 5	Datengeheimnis
§ 6	Unabdingbare Rechte Betroffener
§ 33 § 34 § 35	Rechte der Betroffenen
§ 42a	Informationspflichten

Datensicherheit

§ 9	Technische und organisatorische Maßnahmen

Auftragsdatenverarbeitung

§ 11	Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag; Kontrolle

Audit-Grobplan (Auszug)

Legende: E: Entscheidungsverantwortung, D: Durchführungsverantwortung,
M: Mitwirkungspflicht, I: muss informiert werden

Themen/Zuständigkeiten		VS	DSB	Produktion	Entwicklung	Service & Vertrieb	Admin.	DV
Besondere Formen des Umgangs mit personenbezogenen Daten								
§ 6b	Beobachtung öffentlicher Räume mit Video		M				D	
§ 6c	Mobile personenbezogene Speicher-/Verarbeitungsmedien		M	D				M
§ 9a	Datenschutz-Audit	I	D	M	M	M	M	M
Zulässigkeit/Rechtsgrundlage								
§ 3a	Datenvermeidung/-sparsamkeit		E	M	M	M	M	D
§ 4	Zulässigkeit Datenerhebung, -verarbeitung, -nutzung		E	M	M	M	M	D
§ 28 für	Datenerhebung/-verarbeitung eigene Zwecke		E	M	M	M	M	D
§ 32	Datenerhebung, -verarbeitung für Zwecke des Beschäftigungs-verhältnisses		M	M	M	M	E	D
§ 4a	Einwilligung		I		D	D	D	

Datenschutz-Zertifizierung

Bestätigung der gesetzes-konformen Umsetzung des Datenschutzes durch unabhängiges Prüfinstitut

Maßstab: BDSG

Auditierung im Dreijahresrhythmus mit jährlichen Überwachungsaudits

Erstauditierung: 2006

Wiederholungsaudit: 2009

ZERTIFIKAT

Die

DQS GmbH

Deutsche Gesellschaft zur Zertifizierung von Managementsystemen

bescheinigt hiermit, dass das Unternehmen

DATEV

DATEV eG

Paumgartnerstraße 6-14
90429 Nürnberg

für den Geltungsbereich

Zentrale in Nürnberg, einschließlich der Areale DATEV I-IV,
des DATEV-Informationszentrums Nürnberg
und der im Anhang gelisteten DATEV-Niederlassungen

den

Datenschutz
nach den Vorgaben aus dem

Bundesdatenschutzgesetz (BDSG)
Ausgabe 14. August 2009

gesetzeskonform gestaltet und wirksam umgesetzt hat.

Durch ein freiwilliges Datenschutzaudit gemäß § 9a BDSG,
dokumentiert in einem Bericht, wurde dieser Nachweis erbracht.

Das Unternehmen ist berechtigt, das nachstehende Datenschutz-Gütesiegel
gemäß den festgelegten Regeln zu nutzen

Dieses Zertifikat ist gültig bis	2012-11-10
Zertifikat-Registrier-Nr.	337181 GP
Frankfurt am Main	2009-11-11

Ass. iur. M. Drechsel — Dipl.-Bw. [illegible]

GESCHÄFTSFÜHRER

60433 Frankfurt am Main, August-Schanz-Straße 21

ISMS nach ISO 27001

Bestätigung der gesetzeskonformen Umsetzung des Datenschutzes durch unabhängiges Prüfinstitut

Aspekt Datensicherheit:

Zertifizierung des ISMS nach ISO 27001, Scope DATEV-RZ

Auditierung im Dreijahresrhythmus mit jährlichen Überwachungsaudits

Erstauditierung: 2010

Förderbegutachtung in 2011

öffentlich hinterlegt:
www.datev.de/datenschutz

ZERTIFIKAT

Die
DQS GmbH
Deutsche Gesellschaft zur Zertifizierung von Managementsystemen

bescheinigt hiermit, dass das Unternehmen

DATEV eG
Paumgartnerstraße 6-14
90429 Nürnberg

ein Informationssicherheits-Managementsystem
eingeführt hat und anwendet.

Geltungsbereich:
DATEV Rechenzentrum

Durch ein Audit, dokumentiert in einem Bericht, wurde der Nachweis erbracht,
dass das Managementsystem die Forderungen des folgenden Regelwerks erfüllt:

ISO / IEC 27001 : 2005

Zertifikat-Registrier-Nr.	337181 ISMS
Zertifizierungsdatum	2010-12-08
Gültig bis	2013-12-07

Michael Drechsel
Geschäftsführer

Jan Böge
Geschäftsführer

August-Schanz-Straße 21, 60433 Frankfurt am Main

Auftragsdatenverarbeitung bei DATEV

Vielen Dank für die Aufmerksamkeit!

Noch Fragen?

Zukunft gestalten. Gemeinsam.