udis

Ulmer Akademie für Datenschutz und IT-Sicherheit
gemeinnützige Gesellschaft mbH

Ausbildung zu zertifizierten fachkundigen Datenschutz-beauftragten nach dem Ulmer Modell

Seminarplan 2018/2019

udis, die Ulmer Akademie für Datenschutz und IT-Sicherheit ist eine gemeinnützige Gesellschaft in Ulm, die sich auf die Aus- und Weiterbildung im Bereich des Datenschutzes und der Datensicherheit spezialisiert.

Flaggschiff dieser Aus- und Weiterbildung ist die Ausbildung von **zertifizierten fachkundigen Datenschutzbeauftragten nach dem Ulmer Modell.** Diese wurde als erste in Deutschland überhaupt vor nunmehr 30 Jahren in Ulm gestartet (deshalb „Ulmer Modell“). Das war zu einer Zeit, als die Computer sich auf Schreibtischformat verkleinerten, vom Internet aber noch keine Rede war. Durch Nachdenken waren damals schon beim Handeln mittels Computer konkrete Gefahren irgendwie zu erahnen, auch wenn sie mit den menschlichen Sinnen nicht wahrnehmbar sind.

Was mit den menschlichen Sinnen nicht wahrnehmbar ist, ist für uns aber nicht wirklich „wirklich“. Dieses Handeln findet in einer Scheinwelt statt, eben in einer „virtuellen“ Welt. Und doch hat dieses Handeln sehr reale Konsequenzen und ist deshalb mit sehr realen Gefahren verbunden. Weil diese Gefahren sich aber in einer virtuellen Welt ergeben, wird nicht wie in der realen Welt, von vorneherein versucht, diesen Gefahren zu begegnen. Risiken in virtuellen Welt haben die Tendenz unterschätzt oder gar ignoriert zu werden: „Bei uns ist noch nie etwas passiert“.

In Ulm überlegte man sich schon in den frühen achtziger Jahren, wie man solchen virtuellen Bedrohungen gerecht werden könnte*). So kam man auf die Idee, „Blindenhunde“ für diese Informationsgesellschaft auszubilden, so dass über diese das nicht Wahrnehmbare durch Einsatz bestimmter Methoden und Verfahren dann doch systematisch erkennbar wurde. Das führte dann zur Ausbildung von zertifizierten fachkundigen Datenschutzbeauftragten nach dem Ulmer Modell. Mit dem Fortschreiten der Informationstechnik haben sich die Inhalte der Ausbildung in diesen Jahren stark verändert. Nicht jedoch die Struktur. Nach wie vor dauert ein solches Seminar 16 Tage, die auf drei Wochen innerhalb von etwa drei Monaten verteilt werden und mit einer mehrstündigen schriftlichen Fachkunde-Prüfung abgeschlossen werden.

Da sich die Informationstechnik auch weiterhin rasant fortentwickeln wird, dürfte auch die Fachkunde von zertifizierten Datenschutzbeauftragten schnell verblassen. udis bietet deshalb eine Reihe so genannter **Refresher-Seminare** an, durch die man hier auf dem Stand der Technik bleiben kann. Durch das **Gütesiegel udis^{zert}** (siehe letzte Seite) lässt sich nachweisen, dass auch viele Jahre nach Abschluss einer Datenschutzausbildung bei udis die Fachkunde immer noch up to date ist.

*) In der Neurophysiologie der Universität Ulm beschäftige man sich zu dieser Zeit unter anderem mit der informationstheoretischen Analyse der menschlichen Sinne. Die hierbei eingesetzten Verfahren entstammten der damals hochaktuellen Kybernetik (engl.: Cybernetics). Seitdem ist alles „Cyber“, was sich in der virtuellen Welt abspielt. So wird die virtuelle Welt zum Cyberspace und Verbrechen in der virtuellen Welt zum Cybercrime.

Woche 1

Grundlagen: Informationstechnik und Persönlichkeitsrecht

Prof. Dr. Gerhard Kongehl

(16 Unterrichtseinheiten à 45 Min.)

1. Einführung in den Datenschutz

1.1 Von der Erfindung der Fotografie zur EU-Datenschutzgrundverordnung

- Die Entdeckung des Rechts auf Privatheit
- Von der Ehre zum Persönlichkeitsrecht
- Auf dem Weg zu einer Gesetzgebung bei der Verwendung von personenbezogenen Daten
- Das erste Datenschutzgesetz der Welt
- Datenschutzgesetze in Deutschland
- Das Recht auf informationelle Selbstbestimmung
- Die EG Datenschutzrichtlinie 95/46/EG
- Die Charta der Grundrechte der EU
- Das Urteil des EuGH zum Safe Harbor Verfahren
- Die EU-Datenschutzgrundverordnung

1.2 Unterschiede zwischen Datenschutz und IT-Sicherheit

2. Wirklichkeit und Computerwelt
Risiken der Datenverarbeitung sind oft nicht wirklich „wirklich"

2.1 Begrenzte Wahrnehmbarkeit von technisch bedingten Risiken
2.2 Wem gehören eigentlich meine Daten?
2.3 Der anständige Bürger: Kann seine Daten problemlos jeder haben?
2.4 Änderungen der Funktionalität, die niemand bemerkt
2.5 Kriminelles Handeln ohne Unrechtsbewusstsein
2.6 Mein Schicksal in den Fängen der Algorithmen
2.7 Der Konflikt zwischen Datenschutz und Sicherheit

3. Was ist eigentlich Datenschutz genau?
Datenschutz ist weit mehr als nur Schutz von Daten

3.1 Persönlichkeitsrecht
3.2 Menschenwürde
3.3 Freie Entfaltung der Persönlichkeit
3.4 Recht auf Selbstdarstellung in der Gesellschaft
3.5 Recht auf informationelle Selbstbestimmung
3.6 Recht auf Gewährleistung der Vertraulichkeit und Integrität
3.7 Datenschutz als Verfahrensschutz
3.8 Personenbezogene Daten
3.9 Datenschutz und Schweigepflicht

4. Computerumgang und Persönlichkeitsrecht
Datenschutz als Schutz vor Verfahren, mit denen das Persönlichkeitsrecht beeinträchtigt werden kann

4.1 Datenschutz als Schutz von personenbezogenen Daten
4.2 Datenschutz als Schutz vor unzulänglichen Datenmodellen
4.3 Datenschutz und informationelle Gewaltenteilung
4.4 Datenschutz und das Kontextproblem
in der personenbezogenen Datenverarbeitung
4.5 Datenschutz und das Validitätsproblem
in der personenbezogenen Datenverarbeitung
4.6 Das Recht auf freien Informationszugang
4.7 Nachhaltigkeit der personenbezogenen Datenverarbeitung

Woche 1:

Recht 1: Datenschutz und Computerrecht

Alexander Filip

(16 Unterrichtseinheiten à 45 Min.)

1. Rechtsgrundlagen des europäischen und deutschen Datenschutzrechts

- Warum Datenschutz?
- Hinweis auf WPs der Artikel-29-Gruppe
- Europäisches Primärrecht
- EU-grundrechtliche Vorgaben zum Datenschutz
- EU-Grundrechtecharta
- Europäisches Sekundärrecht
  - Überblick
  - EG-Datenschutzrichtlinie von 1995
  - E-privacy-Richtlinie
  - Datenschutz-Grundverordnung

2. Vorgaben des deutschen Grundgesetzes zum Datenschutzrecht

- Grundgesetz: Grundrecht auf informationelle Selbstbestimmung
- Datenschutz als Europarecht

3. Überblick über Datenschutz-Grundverordnung (DSGVO) und Abweichungen durch BDSGneu

- Überblick zur DSGVO
- Wichtigste Auswirkungen der DSGVO für die Anwender
- Modifikationen der DSGVO durch BDSGneu?

4. Anwendungsbereich von DSGVO und BDSGneu

- DSGVO: sachlicher Anwendungsbereich
- Personenbezogene Daten
- Verarbeitung
- DSGVO: räumlicher Anwendungsbereich
- Problem: Abweichungen vom Anwendungsbereich der DSGVO durch BDSGneu?
- Zum Vergleich: Räumlicher Anwendungsbereich des BDSGalt
- Regulierungsziel des Marktortprinzips der DSGVO

5. Zentrale Begriffe und Strukturen des Datenschutzrechts

- Personenbezogene Daten (Art. 4 Nr. 1)
- Besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1)
- Betroffene Person (Art. 4 Nr. 1)
- Verarbeitung (personenbezogener Daten) (Art. 4 Nr. 2)
- Verantwortlicher (Art. 4 Nr. 7)
- Auftragsverarbeiter (Art. 4 Nr. 8)
- Empfänger (Art. 4 Nr. 9)
- Dritter (Art. 4 Nr. 10)

6. Grundsätze der Verarbeitung personenbezogener Daten (Art. 5 DSGVO)

- Rechtmäßigkeit
- Verarbeitung nach Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung (begrenzte Speicherdauer)
- Integrität
- Vertraulichkeit
- Rechenschaftspflicht

7. Datenschutz-Folgenabschätzung (DSFA)

- Überblick
- Erforderlichkeit einer DSFA
- Durchführung der DSFA
- Konsultation der Aufsichtsbehörde
- Zusammenfassung DSFA + Konsultation

8. Übermittlung personenbezogener Daten in Drittländer

- Übersicht
- Fazit zum Vergleich BDSGalt / DSGVO
  - Einiges bleibt beim Alten
  - Einiges ist neu
- Zusammenfassung der Anforderungen an Übermittlungen in Drittländer
- Angemessenes Datenschutzniveau im Zielland
- Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules)
- Codes of Conduct (genehmigte Verhaltensregeln)
- Zertifizierungsmechanismen, Datenschutzsiegel, - prüfzeichen
- Standarddatenschutzklauseln
- Ausnahmetatbestände
- Übermittlung aufgrund Entscheidungen von Gerichten/Behörden eines Drittlandes
- Übermittlungen in die USA
  - Überblick
  - EU-US Privacy Shield
- Auswirkungen des Schrems-Urteils

Woche 1:

Praxis1: Datenschutzmanagement und Mediendatenschutz

RA Dr. Claus-Dieter Ulmer

(8 Unterrichtseinheiten à 45 Min.)

1. Die Funktion des Datenschutzbeauftragten nach DSGVO und BDSGneu

- Der Wandel der Rahmenparadigmen für den Datenschutzbeauftragten
- Die Notwendigkeit zur Benennung eines Datenschutzbeauftragten
- Die Fachkunde des Datenschutzbeauftragten
- Die Stellung des Datenschutzbeauftragten im Unternehmen
- Weisungsfreiheit und Unabhängigkeit und organisatorische Anbindung
- Die Aufgaben des Datenschutzbeauftragten
- Maßnahmen in der Krise und zur Vermeidung einer Krise
- Exkurs: Die Verarbeitungsverzeichnisse

2. Datenschutzmanagement im Unternehmen

- Elemente von Risikomanagementsystemen
  - Organisation, Regelungsrahmen, Umsetzung, Kontrolle
- Die Datenschutz-Organisation – Varianten für die Steuerung mehrerer Einheiten
- Strukturelle Grundlagen für das Datenschutzmanagement
- Das Datenschutz-Management-Konzept
  - Gliederung und Inhalte
- Die Regelungsgeber-Funktion
- Maßnahmen zur Implementierung von Regelungen
  - Organisatorische, prozessuale, Schulungs- und Awareness-Maßnahmen
- Kontrollmaßnahmen der Datenschutz-Organisation
- Die Datenschutz-Folgenabschätzung in der Unternehmensprozesslandschaft
- Organisationsprüfungen sowie Beratungs- und Kontrollbesuche
- Der Wertbeitrag der Datenschutz-Organisation für ein Unternehmen

3. Der Datenschutz in den Telemedien und der Telekommunikation

- Gesetzliche Grundlagen des Telemediengesetzes (TMG)
  - Einzelne Regelungen
  - Die Pflichten der Diensteanbieter
  - Die elektronische Einwilligung – confirmed opt in und double opt in
  - Weiterverarbeitungstatbestände – Verwendung pseudonymer Daten
  - Datenschutz im Kundenangang über elektronische Medien (Beispielsfälle)
  - Datenschutz bei der Betrachtung von Kunden (Beispielsfälle)
- Gesetzliche Grundlagen des Telekommunikationsgesetzes (TKG)
  - Einzelne Regelungen
  - Fernmeldegeheimnis
  - Weiterverarbeitung von Daten – Verkehrsdaten und Standortdaten
- Voice over Internet Protocol (VOIP)
- Exkurs: Telekommunikation – Telemedien – Cloud Computing – Internet of Things … Welches Recht kommt zur Anwendung?
- Aktueller Stand des Gesetzgebungsprozesses zur ePrivacy Verordnung

Woche 1:

Praxis 2: Workshop: Grundlagen der Selbstdarstellung und Öffentlichkeitsarbeit im Datenschutz

Klaus Jancovius und Partner(in)

(8 Unterrichtseinheiten à 45 Min.)

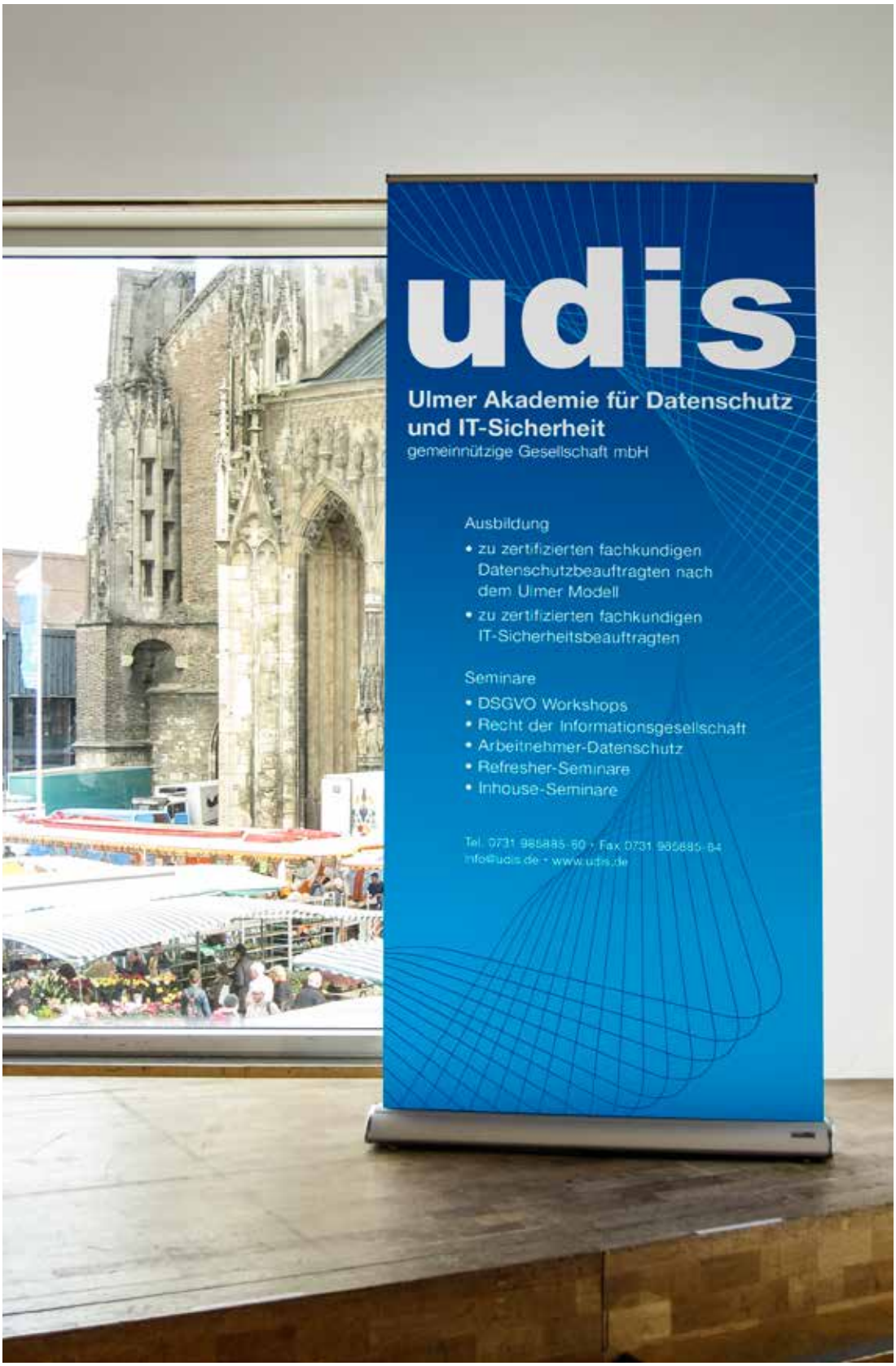
Wie kann man den Datenschutz in Unternehmen, Behörden, Institutionen bei Kunden professionell und wirksam darstellen und vertreten? Darum geht es in diesem Workshop.

Die Teilnehmer/innen lernen, die positiven Seiten des Datenschutzes herauszustellen, Vorteile und Bedeutung in unserer vernetzten Welt zu erklären, ohne dabei die Herausforderungen zu verschweigen, die der Datenschutz auch hervorbringen kann.

- Die Teilnehmenden erleben und erkennen, welche Bausteine eine persönliche Kommunikation, im Gespräch, im Meeting, in einer Konferenz, bei einem Kunden oder einem Chef/in erfolgreich machen:
  - Klare Botschaften
  - Verständliche Sprache und Formulierungen, Vergleiche und Bilder
  - Überzeugender Auftritt in Körpersprache und Ausstrahlung
- Die TN arbeiten in praxisnahen Übungen direkt mit diesen Bausteinen vor der Kamera.
- Die TN können über die Videoaufnahmen einen eigenen Blick auf sich werfen, können Stärken und Verbesserungspotenziale erkennen und daran arbeiten.
- Die TN bekommen individuelles Feedback von den Lehrgangs-TN und den Trainern.
- Viele Tipps und Hinweise aus der Praxis

Wie arbeiten wir?

- Kleine Theorie-Bausteine in der ganzen Gruppe
- Einzelübungen vor der Kamera
- Individuelle Auswertung mit den Trainern (langjährige TV-Moderatoren)


udis
Ulmer Akademie für Datenschutz
und IT-Sicherheit
gemeinnützige Gesellschaft mbH
Ausbildung
• zu zertifizierten fachkundigen Datenschutzbeauftragten nach dem Ulmer Modell
• zu zertifizierten fachkundigen IT-Sicherheitsbeauftragten
Seminare
• DSGVO Workshops
• Recht der Informationsgesellschaft
• Arbeitnehmer-Datenschutz
• Refresher-Seminare
• Inhouse-Seminare
Tel. 0731 985685-60 • Fax 0731 985685-64
info@udis.de • www.udis.de

Woche 2:

IT-Sicherheit 1: Privacy by Design

Prof. Dr. Hannes Federrath

(16 Unterrichtseinheiten à 45 Min.)

Schutzziele in Rechnernetzen

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Datenschutz durch Technikgestaltung in der EU-Datenschutzgrundverordnung

- Privacy by Design und Privacy by Default im Artikel 25 DSGVO
- Sicherheit der Datenverarbeitung im Artikel 32 DSGVO
- Systematik

Systemsicherheit

- Physische Sicherheit
- Zugangskontrolle
- Zugriffskontrolle

Malware

- Viren
- Würmer
- Trojanische Pferde

Grundlagen der Kryptographie

- Systematik
- Symmetrische Verfahren
- Asymmetrische Verfahren
- Schlüssellängen

Kryptographie in der Praxis

- Hybride Kryptographie
- Transport Layer Security
- Pretty Good Privacy
- Secure Multipurpose Internet Mail Extensions

Digitale Signatur und Public Key Infrastrukturen

- Zertifizierungsinfrastrukturen
- X.509-Zertifikate und TLS/SSL
- Sichere Signaturerstellungseinheiten

Überwachung in Kommunikationsnetzen

- Überwachung mittels IP-Adressen
- Überwachung mittels Cookies
- Überwachung mittels Fingerprinting-Verfahren

Grundverfahren zum Schutz vor Beobachtung

- Broadcast
- Proxies
- Mix-Netz
- DC-Netz

Schutz vor Beobachtung in der Praxis

- Anonymes Surfen
- Anonyme E-Mail

Woche 2:

IT-Sicherheit 2: Datenschutz und IT-Sicherheit

Dr. Gerhard Weck

(16 Unterrichtseinheiten à 45 Min.)

1. Schadensszenarien: Die Bedrohungssituation

- Umfang der Bedrohungen: Statistiken
- Struktur der Bedrohungen
  - Urheber: Struktur der Hacker-Community
  - Nutzen: Geschäftsmodelle, Industrialisierung
  - Techniken: Viren, Trojaner, Root Kits, Evil Maid
  - Phishing, Pharming, aktive Inhalte
- Netzbasierte Angriffe
  - Vom gezielten Angriff zum Bot-Netz
- Schwachstellen und ihre Ursachen

2. Schutzziele der IT-Sicherheit: ein Sicherheitsmodell

- Begriffe und Zusammenhänge
- Informationstechnik als Werkzeug
- Duale Sicherheit
- Komponenten der Verlässlichkeit / Beherrschbarkeit:
  - Die Sicherheitsziele
  - Ergänzende Datenschutzziele
- Ein semantisches Modell der IT-Sicherheit und seine Ausprägungen
  - Im BDSG
  - In der DSGVO
- Konsequenzen
- „Stand der Technik“ nach DSGVO

3. Sichere Systeme

- Softwarezuverlässigkeit
  - Pufferüberlauf
- Selbstschutz des Systems
  - Schutz der Integrität
  - Ringschutz
  - Virtualisierung
  - Schutz durch Isolation
- Entwicklung sicherer Client-Systeme
  - Reduktion der Angriffsfläche
  - Beispiel: Virtualisierungssystem Qubes OS
  - Weiterentwicklung zu allgemeiner Architektur

4. Sicherheitsmaßnahmen

- Sicherheitsgrundfunktionen
- Zugangskontrolle
- Zugriffskontrolle
- Zuverlässigkeitstechniken
  - Robuste System-Architekturen
  - Sicherheitstechniken / Virtualisierung
  - Ausfallsicherheit durch Redundanz

5. Sicherheitskomponenten

- Systemverwaltung
- Clouds
- Firewalls
- Schutz gegen Abhören
- Intrusion Detection
- Inhaltsfilterung
- Virenschutz
- Schwachstellenscanner

6. Umsetzung: Das Standard-Datenschutz-Modell (SDM)

- Ein neuer Standard für den Datenschutz
  - Zweck: Konzept zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele
  - Anwendungsbereich des SDM
- Zentrale Anforderungen gemäß Art. 32 DSGVO
  - Datenminimierung gemäß Art. 5 Abs. 1 c) / e) DSGVO
  - Gewährleistungsziele gemäß Art. 5 / 16 / 17 / 32 DSGVO
  - Verfahrenskomponenten und Schutzbedarfskategorien
  - Geplante Grundschutz-Bausteine des SDM
- Prüfungsaspekte

7. Sicherheitskonzepte

- Verantwortung für IT-Sicherheit
- Die Bedeutung der Security Policy
- Methodik und Elemente zur Erstellung von IT-Sicherheitskonzepten
- Standardisierte Methoden: IT-Grundschutz
  - Generelle Vorgehensweise
  - Modernisierung – alternative Vorgehensmodelle
  - Einbindung des Datenschutzes gemäß DSGVO
- Risikoanalyse
- Werkzeugunterstützung

8. Sicherheitsorganisation

- Einbindung des Managements
- Sicherheitsprozesse
- Prinzipien: Sicherheit als Prozess
- Der menschliche Faktor
- Schlussfolgerungen

Woche 2:

IT-Sicherheit 3: Praxis des technischen Datenschutzes

Roman Maczkowsky

(8 Unterrichtseinheiten à 45 Min.)

Einführung

1. Sicherheitsrisiken beim Web-Browsen

- Sicherheitsrisiken & Datenschutzprobleme
- „Bug or Feature?“
- Tracking Techniken [Adressiert ePrivacy-VO]
- Pflichten der Website-Betreiber [Adressiert TMG + ePrivacy-VO]
- „Do Not Track“ (DNT) [Adressiert Art. 25 DSGVO-Praxis]
- verbleibende Sicherheitsrisiken

2. Der „Arbeitsplatz-Proxy“

- Die klassische Internet-Anbindung
- Datenzugriff am Arbeitsplatz
- Client als Schnittstellenrechner
- Angriffs-Szenarien
- Risikoabwägung
- Das ReCoBS-Prinzip [Adressiert Art. 32 DSGVO-Praxis]

3. Risikoanalyse mittels Attack-Tree-Modell und Nutzung für die DSFA

- Grenzen der klassischen Risikoanalyse vs. Attack-Tree
- Statistiken und Risiko
- Modellierung von Schwachstellen mittels Attack-Tree
- Risikoanalyse zur Datenschutz-Folgenabschätzung [nach Art. 35 DSGVO]
- Besonderheiten der DSFA

4. Anonymisierung und Pseudonymisierung

- Einschub: Technisch realisierte Gewaltenteilung [Adressiert Art. 25 + 32 DSGVO-Praxis]
- Anonymität im Internet?
- Identität – Pseudonyme – Anonymität
- Pseudonymisierung im BDSG und in der DSGVO [Art. 4 Nr. 5]
- Pseudonymarten

5. Umgang mit Protokoll-Daten

- Pseudonymisiertes Log [Adressiert Art. 25 + 32 DSGVO-Praxis]
- Praxishilfe Auditdaten [Adressiert Art. 25 DSGVO-Praxis]

6. E-Mail & Webdienste (am Arbeitsplatz)

- Open Relays, Spamschutz, Opt-In und Opt-Out
- Nutzung von Webdiensten + Alternativen

7. Word-Dokumenten-Problematik

Woche 3:

Recht 2: Datenschutz und Computerrecht

Dr. Jens Eckhardt / RAin Nicole Michels

(12 Unterrichtseinheiten à 45 Min.)

1. Rechte der betroffenen Person (Artikel 12 ff)

2. Die EU-Datenschutzgrundverordnung, ihre Öffnungsklauseln und das neue Bundesdatenschutzgesetz

- 2.1 Beschäftigten-Datenschutz
- 2.2. Berufs-/Amtsgeheimnisse
- 2.3. Bußgelder, Sanktionsmöglichkeiten aus Sicht der Verantwortlichen und der Auftragsverarbeiter

3. Datenverarbeitungsverbot mit Erlaubnisvorbehalt

- 3.1. Erlaubnistatbestände

4. Datenverarbeitung (DV) nichtöffentlicher Stellen

- 4.1. Vertrag mit betroffenen Personen
- 4.2. Berechtigtes Interesse der Verantwortlichen
- 4.3. DV zum Zwecke der Werbung
- 4.4. Scoring
- 4.5. DV in Auskunfteien,
- 4.6. DV zum Zwecke der Übermittlung
- 4.7. Markt- und Meinungsforschung

5. Automatisierte Einzelentscheidung und automatisierte Abrufverfahren

6. Verarbeitungsverzeichnis (in Ergänzung zu Claus-Dieter Ulmer)

7. Verantwortlichkeit und Rechenschaftspflicht

- 7.1. In Bezug auf die Einhaltung der Grundsätze nach Artikel 5
- 7.2. In Bezug auf die Sicherheit der Verarbeitung (Artikel 32)

8. Meldung von Verletzungen des Schutzes personenbezogener Daten (Artikel 33 und 34)

9. Erwägungsgrund 171 (Weitergeltung bestehender Einwilligungen usw.)

10. Verhaltensregeln und Zertifizierung

Woche 3:

Recht 3: Datenschutzmanagement und Mediendatenschutz

Dr. Jens Jacobi

(4 Unterrichtseinheiten à 45 Min.)

1. Datenschutzrecht und Datenschutzaufsicht in Europa

1.1. Europäischer Datenschutzbeauftragter
1.2. Artikel-29-Gruppe

2. Datenschutzrecht und Datenschutzaufsicht in Deutschland

2.1.Öffentliche Stellen des Bundes (BfDI)
2.2.Öffentliche Stellen der Länder (LfD‘s)
2.3.Nicht-öffentliche Stellen (Datenschutzaufsichtsbehörden)
2.4.Öffentlich-rechtliche Religionsgemeinschaften

3. Die Öffnungsklauseln der DSGVO und das LDSGneu

3.1. Die Sonderregelungen des LDSGneu
3.2. Sonderregelungen des Beschäftigten-Datenschutzes der öffentlichen Stellen in den Ländern

4. Aufgaben, Befugnisse und Rechtsstellung der Kontrollinstanzen

4.1. Kooperationsgremien
4.2. Bußgelder, Sanktionsmöglichkeiten aus Sicht der Aufsichtsbehörden

5. Detailregelungen des neuen BDSG für öffentliche Stellen

5.1. Zulässigkeit des Datenumgangs im öffentlichen Bereich der Länder
5.2. Übermitteln an öffentliche Stellen
5.3. Übermittlungen an nichtöffentliche Stellen, § 18 LDSG
5.4. Übermitteln zu Forschungszwecken
5.5. Übermitteln in Drittstaaten
5.6. Verarbeitung besonderer Kategorien personenbezogener Daten

Woche 3:

Praxis 3: Betriebswirtschaftliches Basiswissen für Datenschutzbeauftragte

Andreas Werther

(8 Unterrichtseinheiten à 45 Min.)

Für Datenschutzbeauftragte ist Grundwissen in der BWL von Bedeutung, da Fragestellungen nach der Verhältnismäßigkeit der eingesetzten Mittel zur täglichen Praxis werden können und die sollten Datenschutzbeauftragte beantworten können bzw. deren Sichtweise in den Diskussionsprozess innerhalb eines Unternehmens fundiert einbringen können. Liegt Budgetverantwortung vor, dann sind Fragestellungen der BWL tägliche Praxis. Bei Fragestellungen zum ökonomischen Einsatz der bereitgestellten Mittel ist Grundwissen der BWL entsprechend nützlich. Wie die kleinen Beispiele zeigen, sollte diese Einführung dazu dienen, einen Überblick über die BWL zu geben und einen Praxisbezug zu den Themenfeldern, welche Datenschutzbeauftragte im Besonderen betreffen, herstellen.

Vorbereitung
Innerhalb der Seminarunterlagen befindet sich eine Kurzzusammenfassung mit folgenden Themen aus der BWL:

- **Betrieb (Unternehmen)**
- **Wirtschaften im Unternehmen**
- **Ökonomisches Prinzip**
- **Erfolgsmaßstab oder Kennzahlen**
- **Rechtsformen der Unternehmen**
- **Unternehmensführung**
- **Organisation**
- **Managementtechniken**
- **Personal**
- **Controlling**

Diese Zusammenfassung dient in erster Linie dazu, kurz in die Themen einzuführen, um vor allem für den Unterricht zu gewährleisten, dass diese Basics allen Teilnehmenden präsent sind und deshalb sollten diese Unterlagen vor dem Unterricht umfänglich durchgearbeitet werden. Später im Rahmen der Tätigkeit als Datenschutzbeauftragte helfen diese Unterlagen natürlich auch, um einen schnellen Überblick über dieses BWL-Thema zu erhalten.

Der Kurs selbst vertieft oder wiederholt teilweise die Kurzzusammenfassung und befasst sich insgesamt mit folgenden Themen:

- **Was ist Wirtschaften?**
- **Einige Kenngrößen der BWL**
- **Das ökonomische Prinzip**
- **Aufgaben Management**
- **Anspruchsgruppen (Stakeholder)**
- **Ziele des Unternehmens**
- **Formalziele/Sachziele**
- **Kennzahlen**
- **Kosten- und Leistungsrechnung**
- **Kostenartenrechnung**
- **Kostenstellenrechnung**
- **Kostenträgerrechnung**

Woche 3:

Praxis 4: Workshop: Datenschutzanalyse anhand der Musterfirma „udiPrax GmbH“

Prof. Dr. Gerhard Kongehl

(16 Unterrichtseinheiten à 45 Min.)

A. Die Musterfirma udiPrax GmbH

Vorstellung der unserer Phantasie entsprungenen Firma „udiPrax GmbH“ und ihrer DV-Systeme, ihrer Auftragsverarbeiter und ihrer sonstigen Dienstleister in aller Welt. In der Beschreibung dieser Firma haben wir eine große Zahl von Datenschutzproblemen versteckt, die für die vorgesehene Datenschutz-Analyse eine Rolle spielen sollen.

B. Datenschutzanalyse der Firma udiPrax GmbH

Entsprechend der Beschreibung der Musterfirma udiPrax (Teil A) sollen die Seminarteilnehmerinnen und Seminarteilnehmer die in dieser Firma vorhandenen Datenschutzprobleme feststellen und entsprechend den Vorschriften der EU-Datenschutzgrundverordnung (DSGVO) bearbeiten. Im Einzelnen geht es dabei um die folgenden Analysen:

1. Das Wichtigste zuerst

1.1 Benennung eines/einer Datenschutzbeauftragten

Überprüfung, ob bei der Firmenkonstellation der udiPrax ein(e) Datenschutzbeauftragte(r) nach Artikel 37 der DSGVO oder einer anderen Rechtsvorschrift benannt werden muss.

1.2 Ermittlung der Zulässigkeitskriterien

Ermittlung der Zulässigkeitskriterien für die einzelnen bei der udiPrax GmbH eingesetzten DV-Verfahren entsprechend den Vorschriften in Artikel 6 Abs. 1 der DSGVO.

2. Grundsätze, Transparenz und Verzeichnis der Verarbeitungstätigkeiten

2.1 Grundsätze der DV nach Artikel 5 der DSGVO

Grundsätzliche Überlegungen der Geschäftsleitung der udiPrax GmbH, wie die Grundsätze in Artikel 5 Abs. 1 der DSGVO in der Firma umzusetzen wären.

2.2 Transparenzgebot und Pflicht zur Dokumentation der DV

– Umgang mit dem Transparenzgebot nach Artikel 5 Abs.1 lit. a und der Pflicht zur Dokumentation aller Verarbeitungstätigkeiten der udiPrax GmbH nach Artikel 30 der DSGVO.
– Vergleich der entsprechenden Vorschriften zwischen dem bisherigen Bundesdatenschutzgesetz (BDSGalt) und der DSGVO.
– Erstellung eines Verzeichnisses nach Artikel 30 der DSGVO für ein konkretes DV-Verfahren der udiPrax GmbH.

3. Datenverarbeitung außer Haus

3.1 Allgemeines

– Ermittlung der Stellen, bei denen die udiPrax GmbH Datenverarbeitung außerhalb des eigenen Hauses (im In- und Ausland) durchführen lässt und auf der Basis welcher Rechtsgrundlagen dies zulässig ist.
– Vergleich entsprechender Vorschriften und Möglichkeiten der Datenverarbeitung außerhalb des eigenen Hauses (Verarbeitung im Auftrag, Standard-Vertragsklauseln, Privacy Shield, Vertrag mit und ohne Genehmigung der Aufsichtsbehörde, Binding Corporate Rules …)
– Datenübermittlung der udiPrax GmbH in sichere und unsichere Drittländer.

3.2 Auftragsverarbeitung innerhalb der EU

– Vergleich der Vorschriften in §11 Abs. 2 Bundesdatenschutzgesetz (BDSG) mit entsprechenden Vorschriften in Kapitel IV der DSGVO.
– Erstellen eines Vertrags nach Artikel 28 Abs. 3 der DSGVO mit einem konkreten Auftragsverarbeiter der udiPrax GmbH.

3.3 Dienstleistung in einem Drittland

– Erstellen eines Vertrags mit einem Dienstleister der udiPrax GmbH nach Artikel 46 Abs. 2c der DSGVO (EU-Standardvertragsklauseln).

4. Datenschutz-Folgenabschätzung

4.1 Ermittlung der Verfahren, die eine Folgenabschätzung erforderlich machen

Die Firma udiPrax GmbH setzt u.a. DV-Verfahren ein, die nach Artikel 35 der DSGVO möglicherweise eine Folgenabschätzung erforderlich machen. Es ist anhand der unter 1.2 erstellten Liste der eingesetzten DV-Verfahren festzustellen, welche der Verfahren das betreffen könnte.

4.2 Durchführung einer Datenschutz-Folgenabschätzung

Für eines dieser betreffenden Verfahren der udiPrax GmbH ist eine Folgenabschätzung entsprechend Artikel 35 Abs. 7 der DSGVO (allerdings aus Zeitgründen in verkürzter Form) durchzuführen.

5. Berechtigungskonzept

Artikel 24 Abs.1 und Artikel 25 Abs. 2 der DSGVO verlangen, dass geeignete technische und organisatorische Maßnahmen getroffen werden, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Zu diesem Zweck sollen u.a. die von den zuständigen Stellen vergebenen Zugriffsrechte der Mitarbeiter überprüft, ggf. verändert und in einem darauf basierenden Berechtigungskonzept dokumentiert werden.

6. Rechte der betroffenen Personen

Die Firma udiPrax hat von Bürgern Briefe erhalten, die bei den Absendern die Vermutung haben aufkommen lassen, dass die Firma udiPrax unrechtmäßig mit deren Daten umgegangen ist. Die Briefe sind entsprechend den Vorschriften von Kapitel III der DSGVO zu beantworten.

7. Beschäftigten-Datenschutz

Der Betriebsrat der Firma udiPrax GmbH möchte mit der Geschäftsleitung der Firma eine Betriebsvereinbarung über den Einsatz einer digitalen Nebenstellenanlage abschließen. Der Betriebsrat lässt sich hierzu von der Datenschutzbeauftragten der udiPrax GmbH beraten. Er legt ihm deshalb eine Liste der Module dieser Nebenstellenanlage vor, mit der Bitte, diese Module nach den Kriterien der Datenschutzgesetzgebung zu beurteilen. Diese Beurteilung wird im Rahmen dieser Aufgabe von den Semiarteilnehmerinnen und Semiarteilnehmern durchgeführt.

Prüfung:

Notizen:

udis^{zert}: Das udis-Gütesiegel zum Nachweis einer Datenschutz-Fachkunde, die auf dem neuesten Stand ist.

Bei udis ausgebildete Datenschutzbeauftragte gelten in Deutschland, vor allem auch bei den Kontrollinstanzen des Datenschutzes, als optimal fachkundig. Absolventinnen und Absolventen dieser Ausbildung möchten deshalb gerne deutlich machen, dass sie bei udis zu zertifizierten fachkundigen Datenschutzbeauftragten ausgebildet worden sind.

Deshalb hat udis das **Gütesiegel udis^{zert}** entwickelt. Durch dieses Gütesiegel sollen alle, die diese Datenschutzausbildung erfolgreich abgeschlossen haben (und damit udis-zertifizierte Datenschutzbeauftragte sind), ihre Datenschutzqualifikation glaubwürdig darstellen können. Etwa gegenüber den Institutionen der Datenschutzkontrolle, gegenüber ihrem Unternehmen, gegenüber ihren Kunden und Geschäftspartnern und natürlich auch gegenüber der Öffentlichkeit.

Das Gütesiegel udis^{zert} hat eine Laufzeit von vier Jahren. Danach muss es durch Teilnahme an einem Refresher-Seminar erneuert werden. Mit der Siegel-Nummer lässt sich auf der udis Webseite feststellen, ob es noch gültig ist.

Ulmer Akademie für Datenschutz und IT-Sicherheit
gemeinnützige Gesellschaft mbH

Sedanstraße 14
89077 Ulm

Geschäftsstelle und Postanschrift:
udis gGmbH
Marlene-Dietrich-Straße 5
89231 Neu-Ulm

Kontakt:
E-Mail: info@udis.de
Webseite: www.udis.de

Bei Fragen können Sie direkt unser Kontaktformular verwenden:
https://www.udis.de/kontakt/formular.php

Wenn Sie sich für ein Seminar anmelden wollen, können Sie unmittelbar unser Anmeldeformular verwenden:
https://www.udis.de/kontakt/anmeldung.php

Telefon: (0731) 985 885 60
Telefax: (0731) 985 885 64

Bürozeiten: Montag bis Freitag von 8:30 Uhr bis 12:00 Uhr
Ansprechpartner:
Prof. Dr. Gerhard Kongehl
Geschäftsführender Gesellschafter und wissenschaftlicher Leiter der udis Ulmer Akademie für Datenschutz und IT-Sicherheit gGmbH

Redaktion: Prof. Dr. Gerhard Kongehl

Titelgestaltung, Layout: Bert Neumann, Büro für Gestaltung, Nürtingen

udis

Ulmer Akademie für Datenschutz und IT-Sicherheit

gemeinnützige Gesellschaft mbH