

## 1.1 Inhalt

<b>1</b>	<b>Wegweiser</b>
1.1	Inhalt
1.2	Stichwortverzeichnis
1.3	Verzeichnis – Mustervordrucke
1.4	Autorenverzeichnis
<b>2</b>	<b>Aktuelle Hinweise</b>
2.1	Facebook-Fanpage-Betreiber sind gemeinsam mit Facebook für die Einhaltung des Datenschutzes verantwortlich
2.2	eIDAS-Verordnung über elektronische Identifizierung und Vertrauensdienste
2.3	Kostenlose Software zur Datenschutz-Folgenabschätzung (PIA-Tool)
2.4	BSI-Lagebericht zur IT-Sicherheit 2018
2.5	Orientierungshilfe „Verbraucherfreundliche Best-Practice bei Apps“ veröffentlicht
2.6	BSI veröffentlicht Mindeststandard für verschlüsselte Internetverbindungen
2.7	Abmahnung von Datenschutzverstößen durch Verbände
2.8	Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards gemäß § 8a Abs. 2 BSIG
2.9	Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen
2.10	KES-Lagebericht zur Sicherheit 2016
2.11	Arbeitspapier Aktualisierung der Firmware eingebetteter Systeme im Internet der Dinge
2.12	NIS-Richtlinie
2.12.1	Wichtige Bestandteile der NIS-Richtlinie
2.13	Arbeitspapiere „E-Learning-Plattformen“ und „Internationale Grundsätze zur Regulierung der nachrichtendienstlichen Informationsbeschaffung“
2.14	Ratgeber zum Beschäftigtenschutz
2.15	Änderungen beim Sozialdatenschutz
2.16	Gesetz zum strafbaren Offenbaren geschützter Geheimnisse bestimmter Berufsgruppen

- 2.17 Vorerst keine Durchsetzungsmaßnahmen gegenüber den zur Vorratsdatenspeicherung verpflichteten Telekommunikationsanbietern
- 2.18 BMWi veröffentlicht Kompass zur IT-Verschlüsselung
- 2.19 Aufsichtsbehörden fordern Opt-in-Lösung für das Tracking

### **3 Grundlegende Anforderungen an die IT-Sicherheit**

- 3.1 Schutzziele
  - 3.1.1 Szenario der Gefährdungen
  - 3.1.2 Grundbedrohungen
  - 3.1.3 Datenschutz durch Technikgestaltung und Voreinstellung
- 3.2 Schadenssoftware
  - 3.2.1 Computerviren
    - 3.2.1.1 Historie
    - 3.2.1.2 Virenarten
    - 3.2.1.3 Verbreitungswege
    - 3.2.1.4 Abwehr- und Vorbeugemaßnahmen
    - 3.2.1.5 Gegenmaßnahmen nach Virenbefall
    - 3.2.1.6 Anforderungen an Antivirenprogramme
    - 3.2.1.7 Virendokumentation
    - 3.2.1.8 Schulungsunterlagen zu Computerviren
    - 3.2.1.9 Checkliste zum Virenschutz
  - 3.2.2 Spam
    - 3.2.2.1 Funktionsweise und Verbreitungswege von Spam-Mails
    - 3.2.2.2 Relevante technisch-organisatorische Sicherheitsmaßnahmen
    - 3.2.2.3 Rechtliche Fragen und datenschutzrechtliche Problematik
    - 3.2.2.4 Empfohlene Schutzmaßnahmen (Lösungsansätze)
    - 3.2.2.5 Schulungsunterlagen zur Spam-Behandlung
  - 3.2.3 Phishing
    - 3.2.3.1 Ziel, Funktionsweise, Verbreitungswege und Erkennungsmerkmale von Phishing-Angriffen
    - 3.2.3.2 Technisch-organisatorische Sicherheitsmaßnahmen
    - 3.2.3.3 Checkliste zum Schutz vor Phishing-Mails
  - 3.2.4 Pharming
    - 3.2.4.1 Checkliste zum Schutz vor Pharming-Angriffen
  - 3.2.5 Spyware
    - 3.2.5.1 Checkliste zum Schutz vor Spyware
  - 3.2.6 Botnetze
    - 3.2.6.1 Checkliste zu Botnetzen
  - 3.2.7 Scareware

- 3.2.7.1 Checkliste zum Schutz vor Scareware
- 3.2.8 Ransomware
  - 3.2.8.1 Checkliste zum Schutz vor Ransomware
- 3.2.9 Backdoor-Programme
  - 3.2.9.1 Checkliste zum Schutz vor Backdoor-Programmen
- 3.3 Grundlegende Datensicherheitsmaßnahmen
  - 3.3.1 Verschlüsselung
  - 3.3.2 Elektronische Signatur
  - 3.3.3 Datenschutzgerechte Protokollierung beim Betrieb von IuK-Systemen
    - 3.3.3.1 Checkliste für eine datenschutzgerechte Protokollierung
    - 3.3.3.2 Betriebs-/Dienstvereinbarung über die Protokollierung bei der automatisierten Verarbeitung personenbezogener Daten
    - 3.3.3.3 Schulungsunterlagen zur Protokollierung
  - 3.3.4 Standard-Datenschutzmodell
- 4 Rechtliche Grundlagen des Datenschutzes und anderer gesetzlicher Vorschriften**
  - 4.1 Europäische Datenschutz-Grundverordnung (DSGVO)
    - 4.1.1 Art. 1 DSGVO: Gegenstand und Ziele
    - 4.1.2 Art. 2 DSGVO: Sachlicher Anwendungsbereich
    - 4.1.3 Art. 3 DSGVO: Räumlicher Anwendungsbereich
    - 4.1.4 Art. 4 DSGVO: Begriffsbestimmungen
    - 4.1.5 Art. 5 DSGVO: Grundsätze für die Verarbeitung personenbezogener Daten
    - 4.1.6 Art. 6 DSGVO: Rechtmäßigkeit der Verarbeitung
    - 4.1.7 Art. 7 DSGVO: Bedingungen für die Einwilligung
    - 4.1.8 Art. 8 DSGVO: Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft
    - 4.1.9 Art. 9 DSGVO: Verarbeitung besonderer Kategorien personenbezogener Daten
      - 4.1.11 Art. 11 DSGVO: Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist
      - 4.1.12 Art. 12 DSGVO: Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person
      - 4.1.13 Art. 13 DSGVO: Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person
      - 4.1.14 Art. 14 DSGVO: Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

- 4.1.15 Art. 15 DSGVO: Auskunftsrecht der betroffenen Person
- 4.1.16 Art. 16 DSGVO: Recht auf Berichtigung
- 4.1.17 Art. 17 DSGVO: Recht auf Löschung („Recht auf Vergessenwerden“)
- 4.1.18 Art. 18 DSGVO: Recht auf Einschränkung der Verarbeitung
- 4.1.19 Art. 19 DSGVO: Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung
- 4.1.20 Art. 20 DSGVO: Recht auf Datenübertragbarkeit
- 4.1.21 Art. 21 DSGVO: Widerspruchsrecht
- 4.1.22 Art. 22 DSGVO: Automatisierte Entscheidungen im Einzelfall einschließlich Profiling
- 4.1.23 Art. 23 DSGVO: Beschränkungen
- 4.1.24 Art. 24 DSGVO: Verantwortung des für die Verarbeitung Verantwortlichen
- 4.2 Inhaltsübersicht zum neuen Bundesdatenschutzgesetz (BDSG)
  - 4.2.1 § 1 BDSG: Anwendungsbereich des Gesetzes
  - 4.2.2 § 2 BDSG: Begriffsbestimmungen
  - 4.2.3 § 3 BDSG: Verarbeitung personenbezogener Daten durch öffentliche Stellen
  - 4.2.4 § 4 BDSG: Videoüberwachung öffentlich zugänglicher Räume
  - 4.2.5 § 5 BDSG: Benennung
  - 4.2.6 § 6 BDSG: Stellung
  - 4.2.7 § 7 BDSG: Aufgaben
  - 4.2.8 § 8 BDSG: Errichtung
  - 4.2.9 § 9 BDSG: Zuständigkeit
  - 4.2.10 § 10 BDSG: Unabhängigkeit
  - 4.2.11 § 11 BDSG: Ernennung und Amtszeit
  - 4.2.12 § 12 BDSG: Amtsverhältnis
  - 4.2.13 § 13 BDSG: Rechte und Pflichten
  - 4.2.14 § 14 BDSG: Aufgaben
  - 4.2.15 § 15 BDSG: Tätigkeitsbericht
  - 4.2.16 § 16 BDSG: Befugnisse
  - 4.2.17 § 17 BDSG: Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle
  - 4.2.18 § 18 BDSG: Verfahren der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder
- 4.3 IT-Sicherheitsgesetz
  - 4.3.1 Gesetzesbestandteile im Einzelnen
  - 4.3.2 Verordnung zur Bestimmung Kritischer Infrastrukturen
  - 4.3.3 2. Korb der BSI-Kritisverordnung in Kraft getreten

- 4.4 Telekommunikationsgesetz (TKG)
    - 4.4.1 Allgemeine Erläuterungen zum TKG
    - 4.4.2 Teil 1: Allgemeine Vorschriften
      - 4.4.2.1 Wichtige Begriffsbestimmungen
  - 4.5 Telemediengesetz (TMG)
    - 4.5.1 Allgemeine Erläuterungen zum TMG
    - 4.5.2 Allgemeine Bestimmungen
    - 4.5.3 Informationspflichten (Anbieterkennzeichnung)
    - 4.5.4 Verantwortlichkeit
    - 4.5.5 Datenschutzbestimmungen
    - 4.5.6 Nähere Hinweise zur Erstellung einer Anbieterkennzeichnung (Impressum)
      - 4.5.6.1 Muster-Impressum
    - 4.5.7 Nähere Hinweise zur Erstellung einer Online-Datenschutzerklärung
      - 4.5.7.1 Beispiel einer Online-Datenschutzerklärung
    - 4.5.8 Elektronische Gästebücher und Internet-Foren
    - 4.5.9 Schulungsunterlagen zu Datenschutzaspekten des Telemediengesetzes
  - 4.6 Safe Harbor – EU-US Privacy Shield
  - 4.7 Landesdatenschutzgesetze
- 5 Abgrenzung IT-Sicherheit und Datenschutz**
- 5.1 Informationssicherheit, IT-Sicherheit, Datensicherheit, Datenschutz: Begriffe, Ziel, Umfang
    - 5.1.1 Datensicherheitsmaßnahmen
    - 5.1.2 Datenschutzmanagement
      - 5.1.2.1 Betriebs-/Dienstvereinbarung zum Datenschutz und zur Datensicherheit
      - 5.1.2.2 Betriebs-/Dienstvereinbarung über die Gewährleistung der Zugriffskontrolle
      - 5.1.2.3 Betriebs-/Dienstvereinbarung für die automatisierte Verarbeitung von Zeiterfassungsdaten
    - 5.1.3 Strategie bei der Auswahl geeigneter Sicherheitsmaßnahmen
      - 5.1.3.1 Checkliste zur Auswahl geeigneter Sicherheitsmaßnahmen
    - 5.1.4 Beispiel eines Maßnahmenkatalogs
      - 5.1.4.1 Checkliste Zugangskontrolle
      - 5.1.4.2 Checkliste Datenträgerkontrolle
      - 5.1.4.3 Checkliste Speicherkontrolle
      - 5.1.4.4 Checkliste Benutzerkontrolle
      - 5.1.4.5 Checkliste Zugriffskontrolle

- 5.1.4.6 Übertragungskontrolle
  - 5.1.5 Schulungsunterlagen zu Datensicherheitsmaßnahmen i. S. d. § 64 Abs. 3 BDSG
  - 5.1.6 IT-Sicherheitsbeauftragter
  - 5.1.6.1 Muster eines Dienstleistungsvertrags für die Bestellung eines IT-Sicherheitsbeauftragten
  - 5.1.6.2 Muster einer Bestellung zum IT-Sicherheitsbeauftragten
  - 5.1.7 Biometrische Systeme
  - 5.2 Kontrollorgane
  - 5.2.1 Datenschutzbeauftragter
  - 5.2.1.1 Schulungsunterlagen zum Datenschutzbeauftragten
  - 5.2.1.2 Bestellung zum betrieblichen Datenschutzbeauftragten
  - 5.2.1.2.1 Anlage zur Bestellung eines betrieblichen Datenschutzbeauftragten
  - 5.2.1.3 Bestellung zum behördlichen Datenschutzbeauftragten
  - 5.2.1.4 Checkliste zum Datenschutzbeauftragten
  - 5.2.1.5 Erstellung eines Tätigkeitsberichts
  - 5.2.1.6 Einzelprobleme
  - 5.2.2 Rechte der betroffenen Person
  - 5.2.2.1 Einwilligung
  - 5.2.2.2 Recht auf Auskunft
  - 5.2.2.2.1 Muster eines Schreibens zur Auskunftserteilung
  - 5.2.2.3 Recht auf Berichtigung
  - 5.2.3 Aufsichtsbehörden
  - 5.2.3.1 Durchführung von Prüfungen
  - 5.3 Folgen von Datenschutzverletzungen
  - 5.4 Datenschutzfreundliche Technologien
  - 5.4.1 Arbeitspapier „Datenschutzfreundliche Technologien“
  - 5.5 Verpflichtung der Mitarbeiter zur Vertraulichkeit
  - 5.5.1 Muster einer Verpflichtungserklärung
  - 5.5.1.1 Muster einer Verpflichtungserklärung im Rahmen einer Auftragsverarbeitung
  - 5.5.2 Merkblatt zur Verpflichtungserklärung
- 6 Sicherheitsmaßnahmen bei Endgeräten**
- 6.1 Sicherheitsmaßnahmen bei Endgeräten
  - 6.1.1 IT-Sicherheitsbelehrung
  - 6.1.2 Orientierungshilfe zur Passwortvergabe, Passwortwahl und Passwortverwaltung

- 6.1.2.1 Checkliste zur Passwortvergabe, Passwortwahl und Passwortverwaltung
- 6.1.3 Orientierungshilfe zur Protokollierung
- 6.1.4 Betriebs-/Dienstvereinbarung für den Einsatz von IuK-Geräten
  - 6.1.4.1 Muster einer Betriebs-/Dienstvereinbarung über Einführung und Anwendung von IuK-Verfahren
- 6.1.5 Trusted Computing
- 6.1.6 Einzelprobleme
- 6.1.7 Mediaplayer
  - 6.1.7.1 Checkliste zu Mediaplayern
- 6.2 Sicherheit bei Personal Computern
  - 6.2.1 Checkliste für den sicheren Einsatz von Personal Computern
  - 6.2.2 Checkliste für den PC-Einsatz im Stand-alone-Betrieb
- 6.3 Datenschutz und Datensicherheit bei mobilen Geräten
  - 6.3.1 Checkliste für den sicheren Einsatz von mobilen Geräten
  - 6.3.2 Einsatz von Smartphones und Tablet-PCs
    - 6.3.2.1 Checkliste für den sicheren Einsatz von Smartphones und Tablet-PCs
    - 6.3.2.2 Sicherheitsmaßnahmen für iOS-Geräte
    - 6.3.2.3 Mustervereinbarung bzgl. der Nutzung privater mobiler Geräte
  - 6.3.3 Einzelprobleme
- 6.4 Datenschutz und Datensicherheit bei USB-Geräten
  - 6.4.1 Checkliste für Sicherheitsmaßnahmen bei USB-Geräten
- 6.5 Datenschutzgerechter Einsatz von Outlook
  - 6.5.1 Schulungsunterlagen zu Outlook
- 6.6 Schutz- und Sicherheitsmaßnahmen für Multifunktionsgeräte
  - 6.6.1 Checkliste für den sicheren Einsatz von Multifunktionsgeräten
- 6.7 Datenschutzrechtliche Aspekte beim Einsatz optischer Speichermedien
  - 6.7.1 Checkliste zum Einsatz optischer Speichermedien
- 6.8 Applikationen (Apps)
  - 6.8.1 Orientierungshilfe zu den Datenschutzerfordernungen an App-Entwickler und App-Anbieter
  - 6.8.2 Checkliste zu Apps
  - 6.8.3 Musterdokumentation einer App-Entwicklung
- 7 Sicherheitsmaßnahmen im lokalen Netzwerk**
  - 7.1 Allgemeines
    - 7.1.1 Netzwerkkarten

- 7.1.2 Netzwerkarchitektur und Kommunikationsprotokolle
- 7.2 Risiken beim Netzbetrieb
- 7.3 Gewährleistung des Datenschutzes und der Datensicherheit im lokalen Netzwerk
  - 7.3.1 Checkliste zur Überprüfung der Sicherheitsmaßnahmen
  - 7.3.2 Einsatz von Fernsteuerungsprogrammen
    - 7.3.2.1 Checkliste zum Einsatz von Fernsteuerungsprogrammen
- 7.4 Erstellung eines Berechtigungskonzeptes
  - 7.4.1 Checkliste zur Erstellung eines Berechtigungskonzeptes
- 7.5 Zugangs- und Zugriffsschutz
- 7.6 Absicherung von Rechenzentren und Serverräumen
  - 7.6.1 Checkliste bezüglich der erforderlichen Sicherheitsmaßnahmen bzw. Serverraum
  - 7.6.2 Fragenkatalog zur Erkennung und Beseitigung von Mängeln und Schwachstellen bezüglich der Sicherheit in einem Rechenzentrum bzw. Serverraum
  - 7.6.3 Checkliste für Maßnahmen zur baulichen und organisatorischen Sicherheit von DV-Komponenten
  - 7.6.4 Schulungsunterlagen zum Schutz von Rechnerräumen und Servern
- 7.7 Sicheres Datenträgerarchiv
  - 7.7.1 Checkliste für ein sicheres Datenträgerarchiv
- 7.8 Einrichtung eines Benutzerservices
  - 7.8.1 Checkliste zum Benutzerservice
  - 7.8.2 Betriebs-/Dienstanweisung zur Einrichtung eines Benutzerservices
- 7.9 Sicherheitsmaßnahmen für das WLAN
  - 7.9.1 Checkliste zum WLAN
- 7.10 Intranet
  - 7.10.1 Schulungsunterlagen zum Datenschutz und zur Datensicherheit im Intranet
  - 7.10.2 Intranet als soziales Netzwerk
- 7.11 Einzelprobleme
  
- 8 Sicherheitsmaßnahmen im Internet**
  - 8.1 Sicherheit im Internet
    - 8.1.1 Sicherheitsrisiken
    - 8.1.2 Sicherheitsmaßnahmen
      - 8.1.2.1 Einsatz von IPv6
      - 8.1.2.2 Schutz vor Denial of Service-Angriffen
        - 8.1.2.2.1 Checkliste zum Schutz vor Denial of Service-Angriffen



- 8.1.2.3 Checkliste für die Anschaffung, die Installation und den Betrieb einer Firewall
- 8.1.2.3.1 Betriebs-/Dienstanweisung für die Einrichtung und den Betrieb von Firewall-Systemen
- 8.1.3 Sicherer Einsatz von Webbrowsern
- 8.1.3.1 Betriebs-/Dienstanweisung für die Browser-Nutzung
- 8.1.3.2 Checkliste zur Browser-Nutzung
- 8.1.4 Einzelprobleme
- 8.2 E-Mail-Sicherheit
- 8.2.1 Rechtliche Aspekte
- 8.2.2 Gefahren der E-Mail-Nutzung
- 8.2.3 Sicherheitsmaßnahmen
- 8.2.4 Nutzung von Web-Mail-Diensten
- 8.2.5 Archivierung von E-Mails
- 8.2.6 Checkliste zur Gewährleistung der E-Mail-Sicherheit
- 8.2.7 Muster einer Betriebs-/Dienstvereinbarung
- 8.2.7.1 Muster einer Einverständniserklärung
- 8.2.8 Einzelprobleme
- 8.3 Sichere Anbindung von Telearbeitsplätzen
- 8.3.1 Muster einer Betriebsvereinbarung zur Telearbeit
- 8.3.2 Muster einer Genehmigung der Telearbeit
- 8.4 Datenschutz bei Suchmaschinen
  
- 9 Spezielle Sicherheitsfragen**
- 9.1 Auftragsverarbeitung
- 9.1.1 Formen der Auftragsverarbeitung
- 9.1.1.1 Entsorgung von Datenträgern
- 9.1.1.1.1 Verfahrensanweisung zur Datenträgervernichtung
- 9.1.1.1.2 Checkliste zur Datenträgervernichtung allgemein
- 9.1.1.1.3 Checkliste zur Datenträgervernichtung in Eigenregie
- 9.1.1.1.4 Checkliste zur Vernichtung von Datenträgern in Form einer Auftragsdatenverarbeitung
- 9.1.1.2 Wartung und Fernwartung
- 9.1.2 Vor- und Nachteile
- 9.1.3 Bereichsspezifische Regelungen
- 9.1.4 Überprüfung der Auftragsverarbeitung
- 9.1.4.1 Dokumentation einer Überprüfung
- 9.1.5 Funktionsübertragung

- 9.1.6 DIN ISO 37500 „Leitfaden Outsourcing“
- 9.1.7 Checkliste
- 9.1.8 Mustervertrag zur Auftragsverarbeitung
  - 9.1.8.1 Mustervertrag zur Fernwartung
- 9.2 Cloud Computing
  - 9.2.1 Checkliste zum Cloud Computing
- 9.3 Voice over IP (VoIP)
  - 9.3.1 Checkliste zu Voice over IP
- 9.4 Radio Frequency Identification (RFID)
  - 9.4.1 Checkliste zum RFID-Einsatz
  - 9.4.2 Einzelprobleme
- 9.5 Big Data
  
- 10 Sicherheitsempfehlungen des BSI**
  - 10.1 Bundesamt für Sicherheit in der Informationstechnik (BSI)
  - 10.2 IT-Grundschutz
    - 10.2.1 IT-Grundschutz-Standards
    - 10.2.2 IT-Grundschutz-Kataloge
  - 10.3 Baustein Datenschutz im IT-Grundschutz
  - 10.4 Technische Richtlinien
    - 10.4.1 Technische Richtlinie TR-01201 De-Mail
    - 10.4.2 Technische Richtlinie TR-03108 Sicherer E-Mail-Transport
  
- 11 Erstellung eines Sicherheitskonzeptes**
  - 11.1 IT-Sicherheitskonzept
  - 11.2 Erstellung einer IT-Sicherheitsleitlinie
  - 11.3 Regelung der Zuständigkeiten und Aufgabenzuordnung
  - 11.4 Analyse der Schutzbedürftigkeit
    - 11.4.1 Kontrollfragen
    - 11.4.2 IT-Strukturanalyse
  - 11.5 Bedrohungs-, Schwachstellen- und Risikoanalyse
  - 11.6 Security Policy
  - 11.7 Umsetzung des Sicherheitskonzeptes
  - 11.8 Fortschreibung und Überprüfung
  
- 12 Überprüfung durch den Datenschutzbeauftragten**
  - 12.1 Durchführung von Kontrollen
    - 12.1.1 Checkliste zur Einhaltung der technisch-organisatorischen Datensicherheitsmaßnahmen
  - 12.2 Verzeichnis der Verarbeitungstätigkeiten

- 12.2.1 Musterformblatt für das Verzeichnis von Verarbeitungstätigkeiten für Verantwortliche
- 12.2.2 Musterformblatt für das Verzeichnis von Verarbeitungstätigkeiten für Auftragsverarbeiter
- 12.3 Datenschutz-Folgenabschätzung
  - 12.3.1 Videoüberwachung öffentlich zugänglicher Bereiche
  - 12.3.2 Videoüberwachung öffentlich zugänglicher Räume gemäß § 4 BDSG
- 12.4 Meldung und Dokumentation von Sicherheitsvorfällen
- 12.5 Informationspflichten
- 12.6 Dokumentations-, Rechenschafts- und Nachweispflichten
- 12.7 Schulung und Sensibilisierung der Mitarbeiter
  
- 13 Aktuelle Rechtsprechung**
  - 13.1 Schutz des Fernmeldegeheimnisses bei abgespeicherten E-Mails
  - 13.2 Kündigung eines EDV-Administrators aufgrund des Missbrauchs von Zugriffsrechten
  - 13.3 Personenbezug dynamischer IP-Adressen
  - 13.4 Gestaltung des „Bestell-Buttons“
  - 13.5 Kündigung aufgrund eines zufälligen (unerlaubten) Zugriffs auf sensible Firmendaten
  - 13.6 Verwertung von Beweisen bei einer verdeckten Videoüberwachung
  - 13.7 Zuordnung einer IP-Adresse zu einem konkreten Internetanschluss
  - 13.8 Klarnamenpflicht bei Facebook bleibt (vorerst)
  - 13.9 Datenschutzverstoß durch Facebook „Like“ Button
  - 13.10 Außerordentliche Kündigung wegen privater Internetnutzung
  - 13.11 Haftung für Urheberrechtsverletzungen bei öffentlich zugänglichem WLAN
  - 13.12 Mitbestimmung bei Einrichtung von Vertretungszugriffen auf dienstliche E-Mail-Postfächer
  - 13.13 Heimliche Überwachung eines Arbeitnehmers mittels Keylogger
    - 13.13.1 Bundesarbeitsgericht bestätigt das Verwertungsverbot bei Überwachung mittels Keylogger
  - 13.14 EuGH: Vorratsdatenspeicherung ist in der Europäischen Union nur zur Bekämpfung schwerer Straftaten zulässig
  - 13.15 Vertragsstrafe für unerwünschte Werbe-E-Mail
  - 13.16 Mitbestimmung des Betriebsrats beim Facebook-Auftritt des Arbeitgebers