Kanzlei LEU

DER PARITÄTISCHE
RHEINLAND-PFALZ | SAARLAND

Datenschutz im mobilen Arbeitsumfeld

ONLINE Arbeitgeberforum, 24. März 2021

Franz Philippe Bachmann M.A.
Berater für Datenschutz

Kanzlei LEU

Leu Rechtsanwaltsgesellschaft mbH

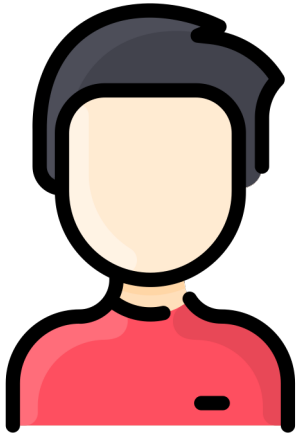
Kanzlei für gemeinnützige Organisationen und Sozialwirtschaft

- Gründung von Vereinen, Gesellschaften, Stiftungen usw.
- Umstrukturierungen, Ausgliederungen, Gremienrecht
- Nationales und internationales Kooperationsrecht
- Datenschutzrecht für gemeinnützige Träger
- Finanzierungen, Fördermittel- und Zuwendungsrecht
- Risiko- und Compliance-Management, Verhaltenskodizes
- Vertragsrecht im gemeinnützigen Bereich
- Schulungen von Vorständen, Geschäftsführungen usw.

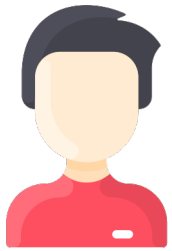

Daten

Kanzlei LEU

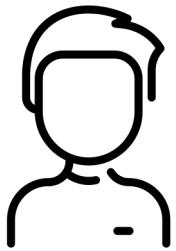
Personenbezogene Daten



Informationen, die sich auf eine natürliche, lebende Person beziehen



Identifizierte Person
Namen, Geburtsdatum, Wohnanschrift, Ausweisnummer, Bürger-Identifikationsnummer, …



Identifizierbare Person
Standortdaten, Kfz-Kennzeichen, IP-Adresse, Bild, Online-Pseudonym, Merkmalskombinationen, …

Kanzlei LEU

Besondere Kategorien

Personenbezogene Daten mit besonderem Schutz

- Ethnische Herkunft
- Politische Meinungen
- Religiöse und weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Genetische Daten
- Biometrische Daten zur eindeutigen Identifizierung
- Gesundheitsdaten
- Sexualleben und sexuelle Orientierung
- Strafrechtliche Verurteilungen und Straftaten

Kanzlei LEU

Weitere sensible Daten

Kritische personenbezogene Daten

- Finanzdaten (z.B. Bankverbindung)
- Sozialdaten (Sozialgeheimnis, Sozialdatenschutz)
- Anvertraute Daten (Kinder- und Jugendhilfe)
- Berufsgeheimnisse (z.B. Ärzte, Sozialpädagogen)
- Daten vulnerabler Personengruppen (z.B. Minderjährige)
- Angriffsvektoren (z.B. E-Mail-Adresse, IT-Schwachstellen)
- Wohnanschrift (besonders bei gefährdeten Personen)
- Zugangsdaten (z.B. IDs, Passwörter, Tokengeneratoren)
- Daten für Identitätsdiebstahl (z.B. Geburtsdatum, Handy)

Kanzlei LEU

Geschäftsgeheimnisse

Beispiele für vertrauliche Daten ohne Personenbezug

- Bewerbungen bei Vergaben und Ausschreibungen
- Gehaltsstrukturen im außertariflichen Bereich
- Sensible Kennziffern, z.B. Krankheitsquote
- Vertragliche Regelungen mit Kooperationspartnern
- Geplante Transaktionen, z.B. Übernahmen
- Angedachte Umstrukturierungen und Reorganisationen
- Compliance-Vorfälle, z.B. Abrechnungsfehler, Datenpannen
- Fehlerverhalten von Beschäftigten, z.B. Übergriffe

Regeln


NJW
Schuldrecht
Familienrecht
StGB
StPO
Der Erbprozess
Erbrecht
Testament und Erbvertrag
Vererben & Erben
BSHG
NZV

Kanzlei LEU

Rechtsgrundlagen

Datenschutz-Grundverordnung (DSGVO)
und bereichsspezifische Regelungen
z.B. E-Privacy-Richtlinie aus 2002,
Ablösung durch E-Privacy-Verordnung geplant

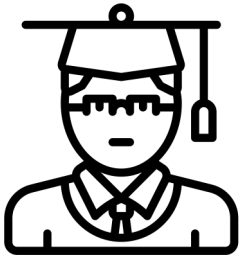
Bundesdatenschutzgesetz (BDSG)
und bereichsspezifische Regelungen
ca. 150 Bundesgesetze,
kirchliche Datenschutzgesetze

Landesdatenschutzgesetze (LDSG)
z.B. Saarländisches Datenschutzgesetz (SDSG)
und bereichsspezifische Regelungen

Kanzlei LEU

Weitere Rechtsgrundlagen

Rechtsprechung
Konkretisierung abstrakter Rechtsnormen
durch Gerichtsurteile

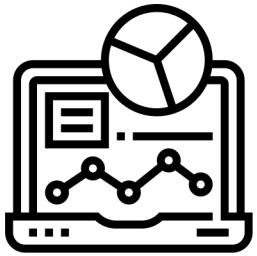


Herrschende Meinung
Interpretationen und Anwendungen
durch Kommentatoren und Aufsichtsbehörden

Stand der Technik
Nach Auffassung von Fachleuten praxisbewährte
Verfahren, Einrichtungen und Betriebsweisen

Kanzlei LEU

Stand der Technik



Kanzlei LEU

Beispiele für Telearbeit

Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium, Stand Februar 2021

OPS.1.2.4.A2 Sicherheitstechnische Anforderungen an den Telearbeitsrechner (B)

Es MÜSSEN sicherheitstechnische Anforderungen festgelegt werden, die ein IT-System für die Telearbeit erfüllen muss.

Es MUSS sichergestellt werden, dass nur autorisierte Personen Zugang zu den Telearbeitsrechnern haben. Darüber hinaus MUSS der Telearbeitsrechner so abgesichert werden, dass er nur für autorisierte Zwecke benutzt werden kann.

OPS.1.2.4.A5 Sensibilisierung und Schulung der Mitarbeiter (B)

Anhand eines Leitfadens MÜSSEN die Mitarbeiter für die Gefahren sensibilisiert werden, die mit der Telearbeit verbunden sind. Außerdem MÜSSEN sie in die entsprechenden Sicherheitsmaßnahmen der Institution eingewiesen und im Umgang mit diesen geschult werden. Die Schulungs- und Sensibilisierungsmaßnahmen für Mitarbeiter SOLLTEN regelmäßig wiederholt werden.

SYS.3.1.A12 Verlustmeldung für Laptops [Benutzer] (S)

Benutzer SOLLTEN umgehend melden, wenn ein Laptop verloren gegangen ist oder gestohlen wurde. Dafür SOLLTE es in der Institution klare Meldewege geben. Wenn verlorene Laptops wieder auftauchen, SOLLTE untersucht werden, ob sie eventuell manipuliert wurden. Die darauf eingesetzte Software inklusive des Betriebssystems SOLLTE komplett neu installiert werden.

Kanzlei LEU

IT-Sicherheit und Datenschutz

IT-Sicherheit ist durch DSGVO eine gesetzliche Anforderung

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“

Art. 32 Abs. 1 DSGVO

Kanzlei LEU

IT-Sicherheit und Datenschutz

Kontinuierliche Aktualisierung und Neubewertung erforderlich

- Stand der Technik
  ⟹ **Dynamik**
- Implementierungskosten
  ⟹ **Wirtschaftlichkeit**
- Eintrittswahrscheinlichkeit, Schwere des Risikos
  ⟹ **Risikobasierter Ansatz**
- Angemessenes Schutzniveau
  ⟹ **Abwägung**

Kanzlei LEU

Grundsätze auch bei Telearbeit

- Rechtmäßigkeit und Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

→ Rechenschaftspflicht

Fallen

Kanzlei LEU

Videokonferenzen

Vor der Videokonferenz

- Auftragsverarbeitung mit Anbieter vereinbaren
- *oder:* System selbst betreiben (Last? IT-Sicherheit?)
- Keine Datenübermittlung in unsichere Drittstaaten, z.B. USA
- Mit Sicherheitseinstellungen vertraut machen

Während der Videokonferenz

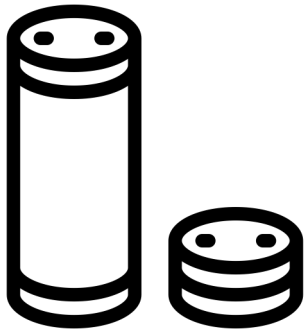
- Unberechtigte Teilnehmer identifizieren und entfernen
- Virtueller Hintergrund oder „Blurring“ aktivieren
- Ende-zu-Ende-Verschlüsselung bei sensiblen Daten
- Keine Aufzeichnung ohne Rechtsgrundlage

Kanzlei LEU

Sprachgesteuerte Assistenten

Beispiele für Smart Speaker

- Amazon Echo
- Google Home
- Apple HomePod
- Hallo Magenta



Abschalten bei mobilem Arbeiten zuhause

- Datenverarbeitung nicht im Gerät, sondern bei Anbieter
- Unbemerkte Datenübermittlung bei Telefonaten
- Intransparente Speicherung und Verarbeitung

Kanzlei LEU

E-Mail

Versand an falschen Empfänger

- Zum Beispiel durch automatische Vervollständigung
- Sofort Empfänger kontaktieren und um Löschung bitten
- Vorgang dokumentieren und weitermelden

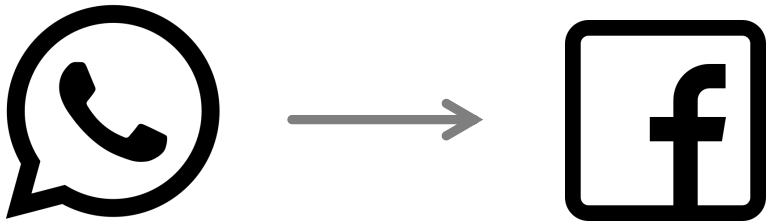
Versand mit offenem Verteiler

- Nur zulässig bei Funktionsadressen, Dienstadressen oder wenn sich Empfänger untereinander kennen und ihre Kontaktdaten
- Sonst Vorgang dokumentieren und weitermelden

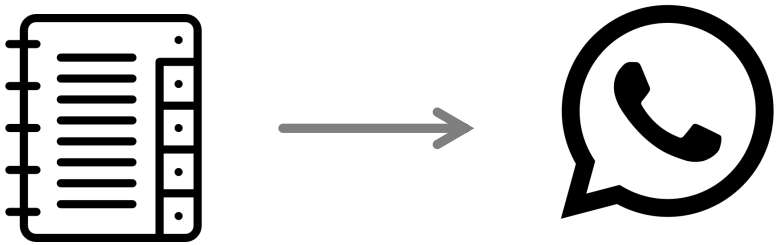
Kanzlei LEU

WhatsApp

Profilbildung und Deanonymisierung



Weiterverarbeitung des Telefonbuchs



Kanzlei LEU

Bring your own device (BYOD)

Möglichst nur betriebliche Endgeräte nutzen, oder sonst…

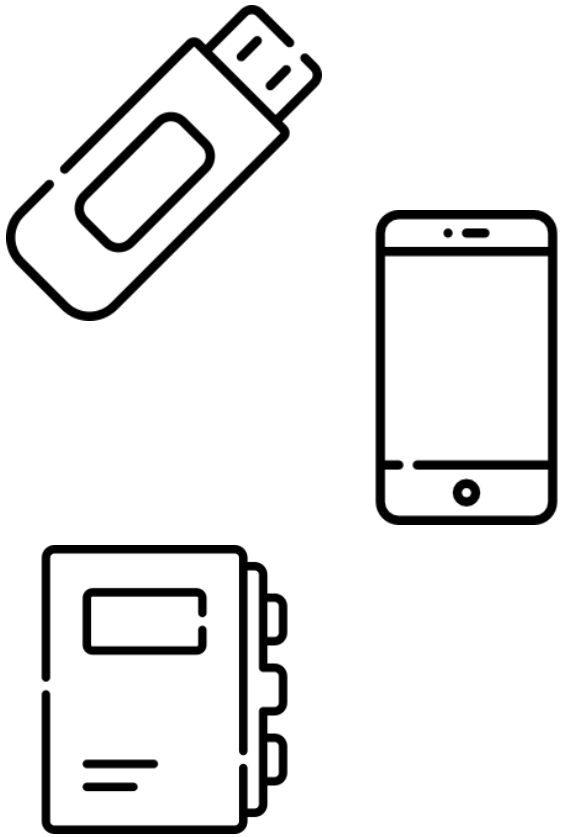
- Trennung von privater und dienstlicher Nutzung
- Containering (virtuelle Umgebung auf z.B. Smartphones)
- Terminalserver mit virtuellen Arbeitsplätzen
- Speicherung auf Server der Organisation über VPN-Verbindung
  oder Speicherung in der betrieblichen Cloud,
  oder Speicherung auf betrieblichem externen Datenträger,
  jedenfalls keine lokale Speicherung (Arbeitsanweisung)
- Keine Nutzung „kostenloser“ Cloud-Dienste,
  insbesondere nicht Speicherung in unsicherem Drittland
- Löschung betrieblicher Daten auf privaten Endgeräten

Kanzlei LEU

Mobile Datenträger

Digitale Datenträger

- USB-Sticks nicht benutzen
- Mobiltelefone verschlüsseln
- Laptops verschlüsseln

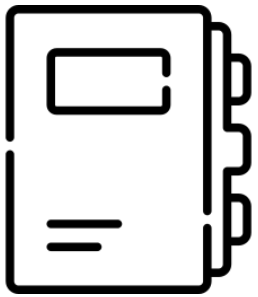


Analoge Datenträger

- Kalender mit Klientendaten
- Papierhafte Unterlagen
- Fotografien

Kanzlei LEU

Papierhafte Unterlagen



Beim Transport sichern

- Verschlossenes, neutrales Behältnis
- Nicht im Auto liegen lassen
- Vorsicht beim Lesen in öffentlichen Verkehrsmitteln

Sicher lagern, im Büro und auch zuhause

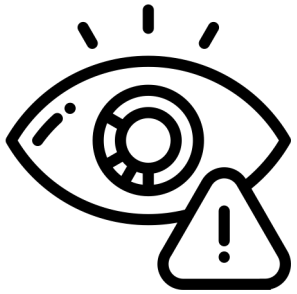
- Schutz abhängig vom Grad der Sensibilität
- Nicht offen herumliegen lassen
- Sauberer Arbeitsplatz: *Clean Desk Policy*

Kanzlei LEU

Öffentliche Verkehrsmittel

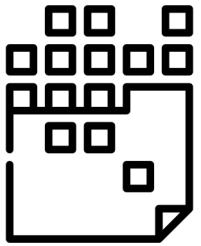
Gefahren bei Benutzung von Bus, Bahn usw.

- Mithören dienstlicher Telefonate
- Mitlesen ausgedruckter Dokumente
- Blick auf Laptop, Tablet, Smartphone
- Verlust von Unterlagen und Geräten



Maßnahmen

- Beschäftigte sensibilisieren
- Sichtschutzfolien für Endgeräte
- Verschlüsselung aller Datenträger

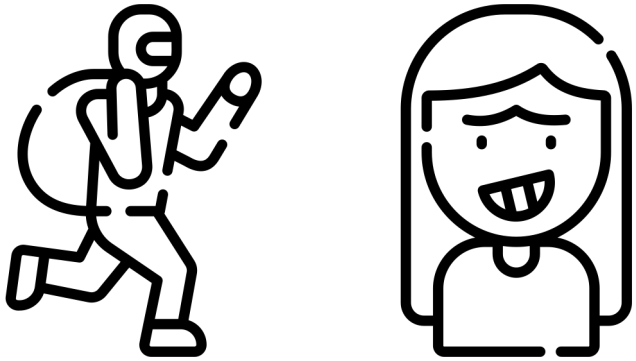


Kanzlei LEU

Verlust von Endgeräten

Mobile IT-Endgeräte gehen verloren

- Laptop
- Tablet
- Smartphone
- Kameras

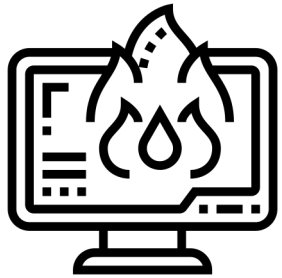


Maßnahmen

- Verschlüsselung aller Datenträger
- Zentrale Verwaltung mobiler Arbeitsgeräte
- Mobile Device Management, inkl. z.B. Remote Wipe

Kanzlei LEU

Verlust von Daten



Datenschutz ist auch Schutz vor Löschung und Vernichtung

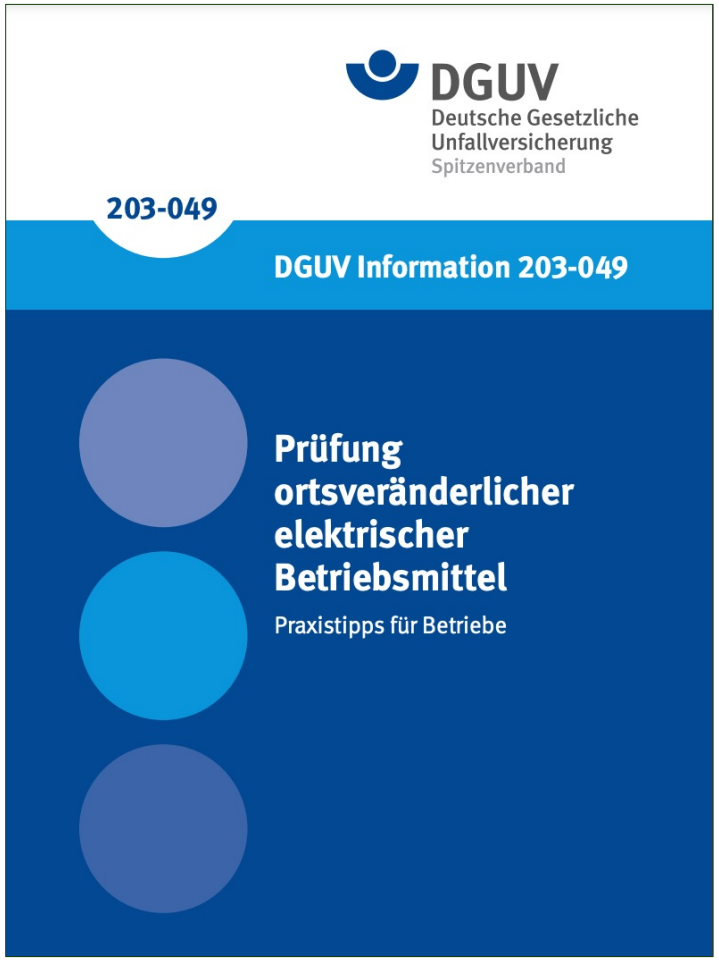
- Originalurkunde, Gesprächsnotiz usw. in Aktenvernichter
- Unbeabsichtigte Löschung von Dateien auf Server
- Starkes Magnetfeld und klassische Festplatte
- Beschädigung oder Zerstörung eines Endgeräts

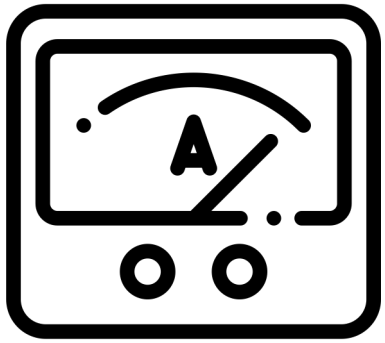
Maßnahmen

- Datensicherung (Backup), Test Wiederherstellung (Recovery)
- Arbeitsanweisung zur Speicherung auf Server bzw. in Cloud
- Prüfung ortsveränderlicher elektrischer Betriebsmittel

Kanzlei LEU

Prüfung elektrischer Betriebsmittel

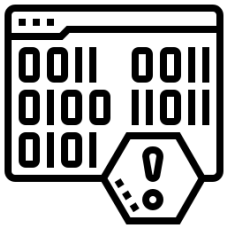





Pannen

Kanzlei LEU

Datenpannen



Verletzung des Schutzes personenbezogener Daten

- Offenbarung gegenüber Unberechtigten
- Zugriffsmöglichkeit für Unberechtigte
- Unplanmäßige Löschung oder Vernichtung

Maßnahmen

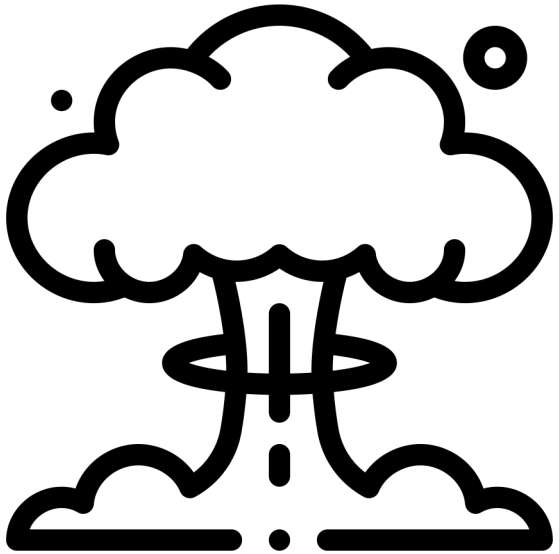
- Meldewege definieren, Beschäftigte schulen
- Jeden Vorfall umfassend dokumentieren
- Ggf. Meldung an Aufsichtsbehörde (Frist: **72 Stunden**)
- Ggf. Information aller Betroffenen (Herausforderung)

Kanzlei LEU

Vorsorge ist billiger als Schaden

Schäden verschiedener Art

- Schadensbehebung
- Behinderung der Arbeit
- Bußgeld wegen Verstoß
- Eintrag ins GZR
- Schadensersatz Betroffene



Zentrale, sehr wirksame Maßnahmen

- Schulungen mit regelmäßiger Wiederholung
- IT-Sicherheit ernsthaft implementieren

Kanzlei LEU

Wir danken für Ihre Aufmerksamkeit.

Ihre Experten für den Dritten Sektor

Leu Rechtsanwaltsgesellschaft mbH
Heinrich-Hoffmann-Straße 3
60528 Frankfurt am Main
Tel.: 069 / 348 731 880
Fax: 069 / 348 731 889
E-Mail: info@kanzlei-leu.de
Web: www.kanzlei-leu.de

Direkter Kontakt für Fragen:
Franz Philippe Bachmann
Tel.: 069 / 348 731 884
E-Mail: fpb@kanzlei-leu.de