Einführung in den technischen Datenschutz

Inhaltsübersicht

Evangelische Kirche in Deutschland
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

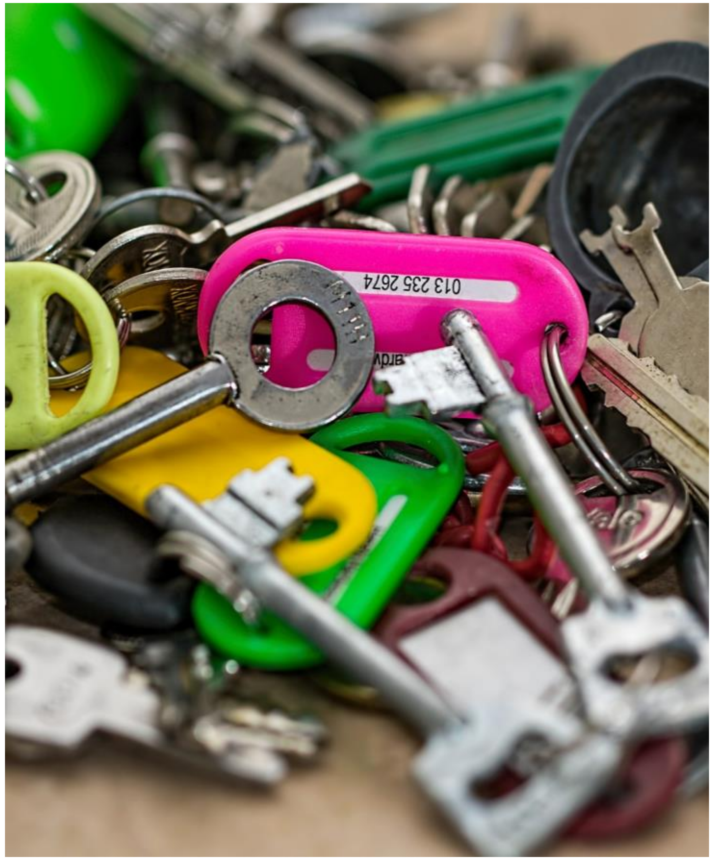
Verschlüsselung

Maßnahmen zum Schutz der Vertraulichkeit

- Absicherung der externen Schnittstellen des Netzwerkes durch eine Firewall
- Aktueller Malware-Schutz auf den Computersystemen im Netz und an den externen Schnittstellen
- Schnelle Reaktion auf bekanntgewordene Schwachstellen
- Physischer Schutz vor unbefugten Zugriffen (TOM: Zugriffskontrolle)
- Nach „Need to know“-Prinzip ausgerichtete Vergabe von Zugriffsberechtigungen
- Systematische Verschlüsselung von sensiblen Dateien
- Organisatorische Maßnahmen müssen die technischen flankieren!
- Alle Maßnahmen zusammen sind elementar, selbst wenn sie nur unzureichend umgesetzt sind.

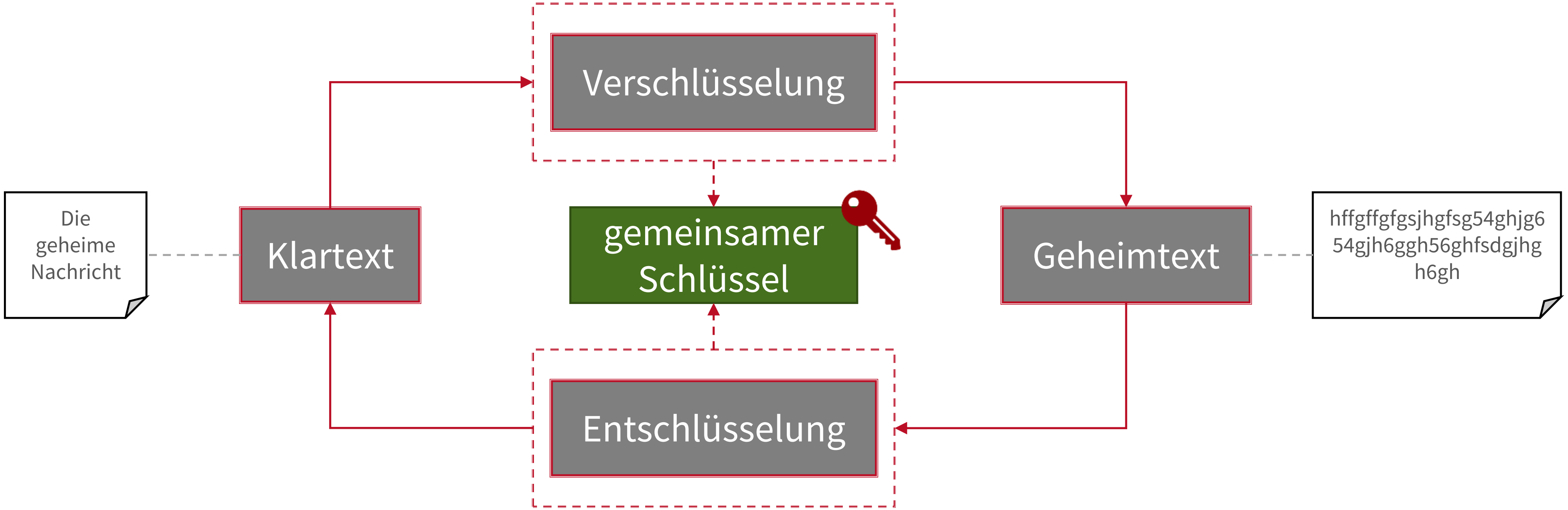
Verschlüsselung

- Wirkt selbst dann, wenn andere Maßnahmen versagen.
- Verschlüsselung ist insbesondere bei der Übertragung von Daten per E-Mail und beim Transport von Speichermedien erforderlich.
- Verschlüsselung trägt bei personenbezogenen Daten dazu bei, die Anforderungen des DSG-EKD zu erfüllen.
  - Zugangs-, Zugriffs- und Weitergabekontrolle
- Verschlüsselung alleine reicht aber auch nicht!
  - Schutz der Authentizität z.B. durch Signaturen
  - Schutz der Integrität
  - Schutz der Verbindlichkeit (Nichtabstreitbarkeit)



Symmetrische Verschlüsselung

- Kommunikationspartner teilen sich einen gemeinsamen, geheimen Schlüssel (im Prinzip ein Passwort).
- Herausforderung: Neben der verschlüsselten Information muss auch der Schlüssel „sicher“ übermittelt bzw. ausgetauscht werden.



Evangelische Kirche in Deutschland

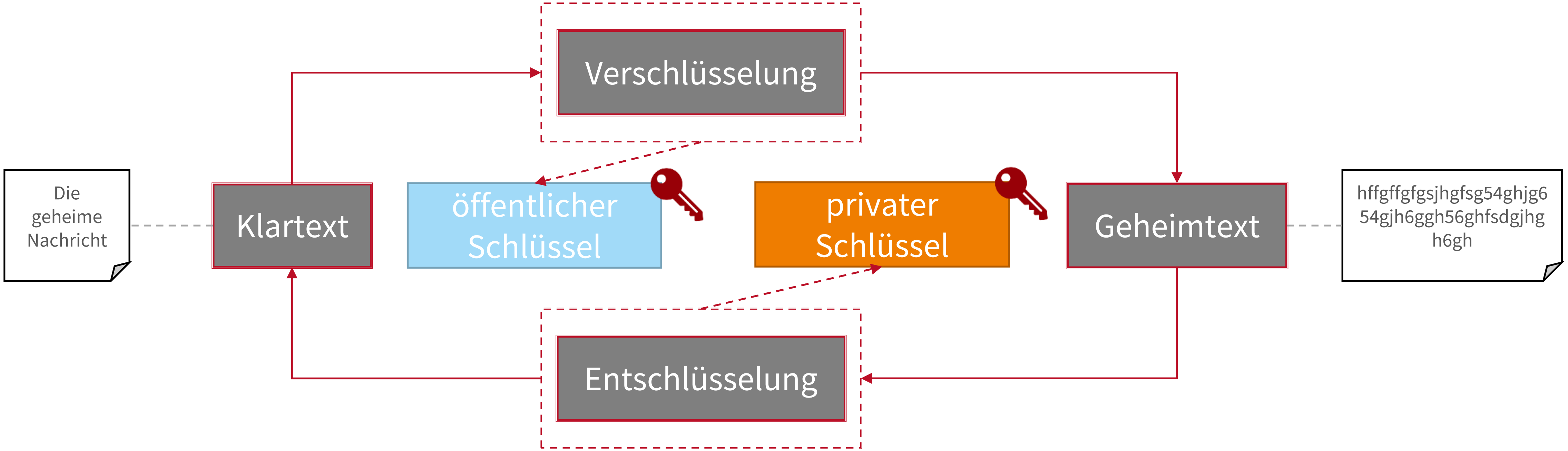
DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Beispiel für symmetrische Verschlüsselung

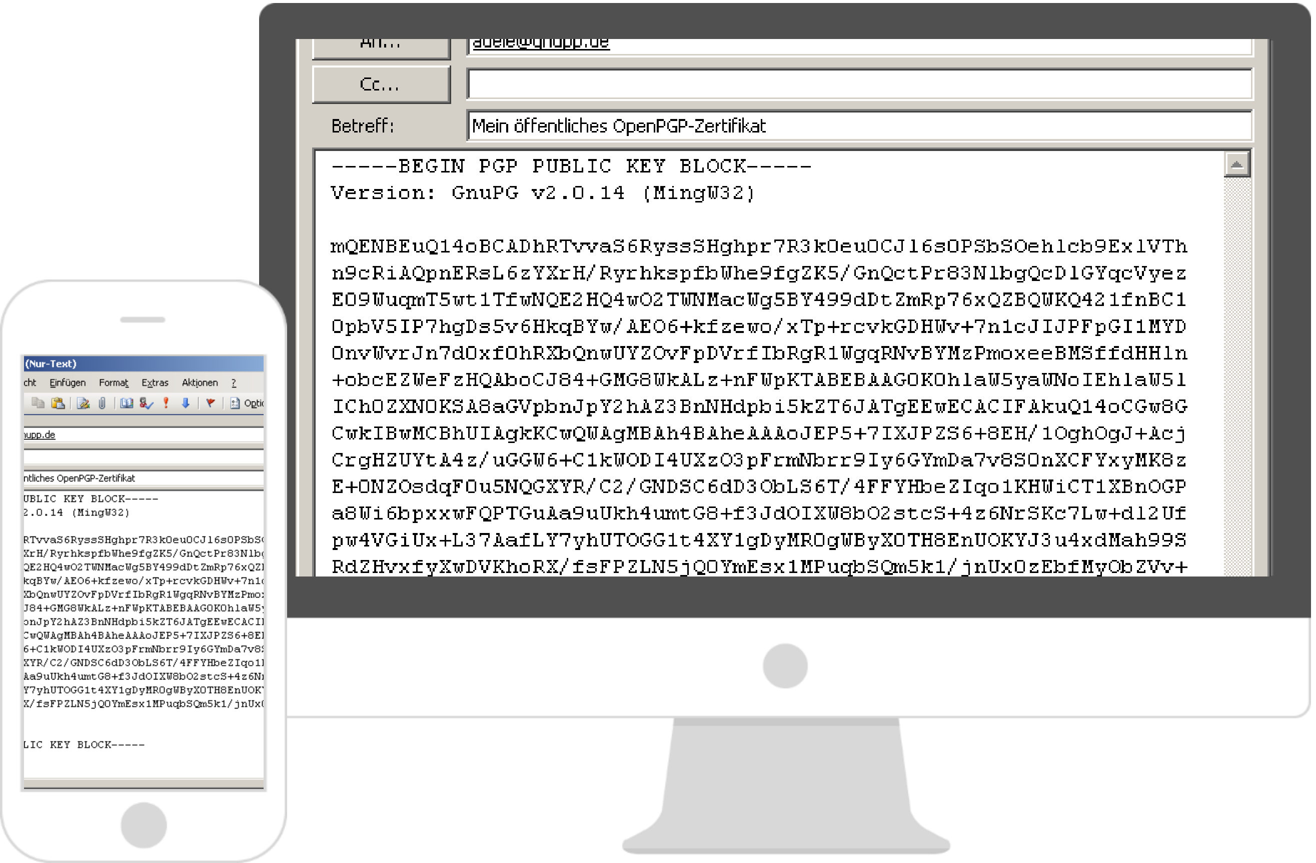
- Nutzung von 7zip zum Verschlüsseln von Dateien und Verzeichnissen auf dem PC

Asymmetrische Verschlüsselung

- Kommunikationspartner haben keinen gemeinsamen geheimen Schlüssel.
- Jeder erzeugt ein Schlüsselpaar: Geheimer Schlüssel (private key) und öffentlicher Schlüssel (public key).



Beispiel für die asymmetrische Verschlüsselung



- Nutzung von Pretty Good Privacy (PGP) oder S/MIME für die Verschlüsselung der E-Mail Kommunikation

Umgang mit USB-Sticks

Sicherer Umgang mit USB-Sticks (1)

- Verschlüsseln der sensiblen Informationen.
  - Kommt ein Stick abhanden, geraten die sensiblen Informationen in die falschen Hände und können missbraucht werden.
  - Bitlocker oder VeraCrypt verwenden, um die Daten vor dem Zugriff Dritter zu schützen oder einen USB-Stick der die Verschlüsselung integriert hat (z.B. G3) nutzen.
- Keine Verwendung von USB-Sticks die aus einer unsicheren Quelle stammen.
  - Häufig nutzen Kriminelle portable Speichermedien, um Schadsoftware wie Viren, Würmer und Trojaner zu verbreiten.
  - USB-Sticks aus unsicheren Quellen müssen daher zuvor an einem Quarantäne Rechner außerhalb des Netzwerkes auf Viren und Schädlinge überprüft werden, bevor sie am Arbeitsplatz genutzt werden können.

Sicherer Umgang mit USB-Sticks (2)

- USB-Sticks sollten immer richtig abgemeldet werden.
  - Wenn der Schreibvorgang noch aktiv ist, kann es zu Datenverlust kommen. Wechseldatenträger werden sicher getrennt, indem in der Taskleiste auf den Menüpunkt „Hardware sicher entfernen“ geklickt wird.
- USB-Sticks sollten nie als einzige Datenquelle genutzt werden.
  - Um bei Verlust oder Defekt des USB-Sticks nicht das Nachsehen zu haben, sollten immer nur Kopien von Dateien darauf gespeichert werden. Die Originale sollten zur Sicherheit auf dem PC oder anderen Speichermedien gehalten werden.
- Daten auf den USB-Sticks richtig löschen.
  - Um Speichermedien restlos von Daten zu befreien, reicht es nicht aus diese einfach zu löschen.
  - Die Informationen sind meist weiterhin auf dem Datenträger hinterlegt und können mit speziellen Programmen in kürzester Zeit wiederhergestellt werden.
  - Es sollte Spezialsoftware verwendet werden, um die Daten effektiv zu löschen oder den USB-Stick zu formatieren.

Technische und organisatorische Maßnahmen

Technische und organisatorische Maßnahmen, § 27 DSG-EKD

§

(1) Die verantwortliche Stelle und der kirchliche Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und einen Nachweis hierüber führen zu können. (…)

Abgrenzung von technischen und organisatorischen Maßnahmen

Technische Maßnahmen

Unter technischen Maßnahmen sind alle Schutzversuche zu verstehen, die im weitesten Sinne physisch umsetzbar sind, wie etwa

- Umzäunung des Geländes
- Sicherung von Türen und Fenstern
- bauliche Maßnahmen allgemein
- Alarmanlagen jeglicher Art
- oder Maßnahmen, die in Soft- und Hardware umgesetzt werden, wie etwa
    - Benutzerkonto,
    - Passworterzwingung,
    - Logging (Protokolldateien) und
    - biometrische Benutzeridentifikation.

Organisatorische Maßnahmen

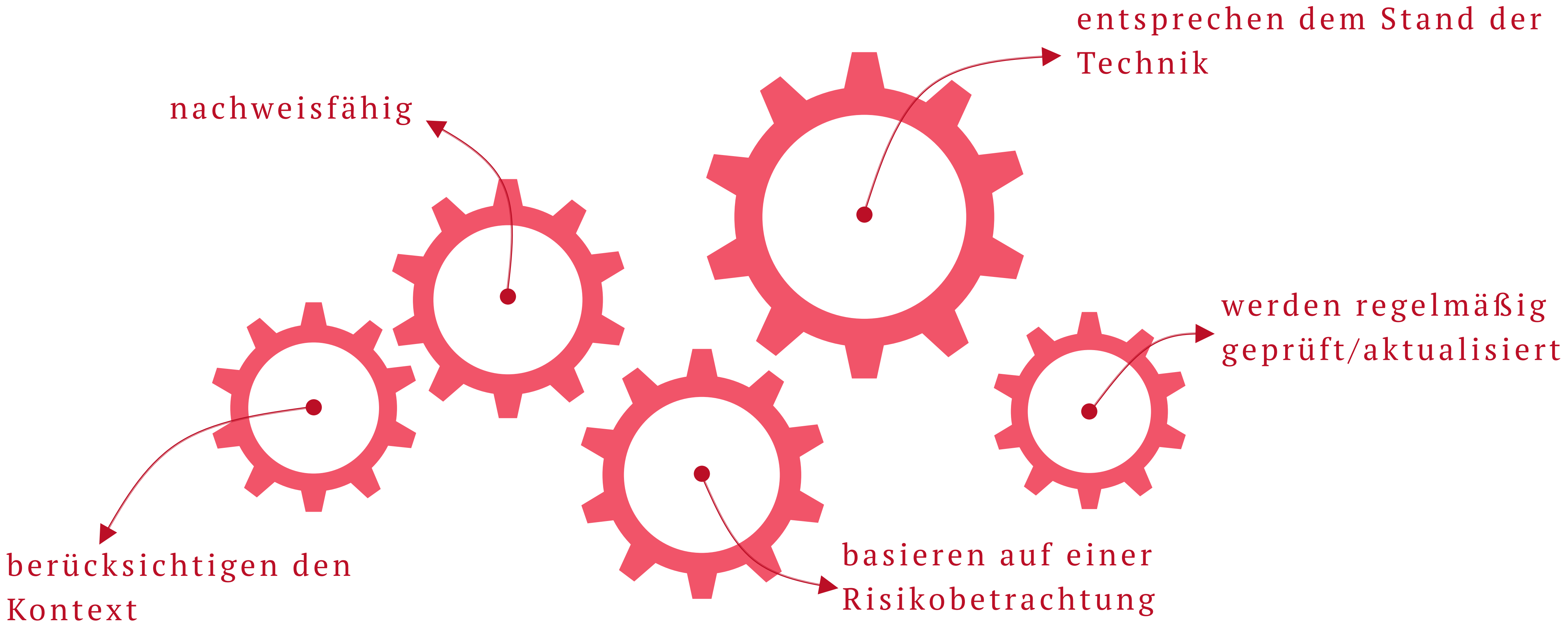
Als organisatorische Maßnahmen sind solche Schutzversuche zu verstehen, die durch Handlungsanweisung, Verfahrens- und Vorgehensweisen und Prozessbeschreibungen umgesetzt werden. Beispiele hierfür sind:

- Besucheranmeldung
- Arbeitsanweisung zum Umgang mit fehlerhaften Druckerzeugnissen
- Vier-Augen-Prinzip und
- festgelegte Intervalle zur Stichprobenprüfungen.

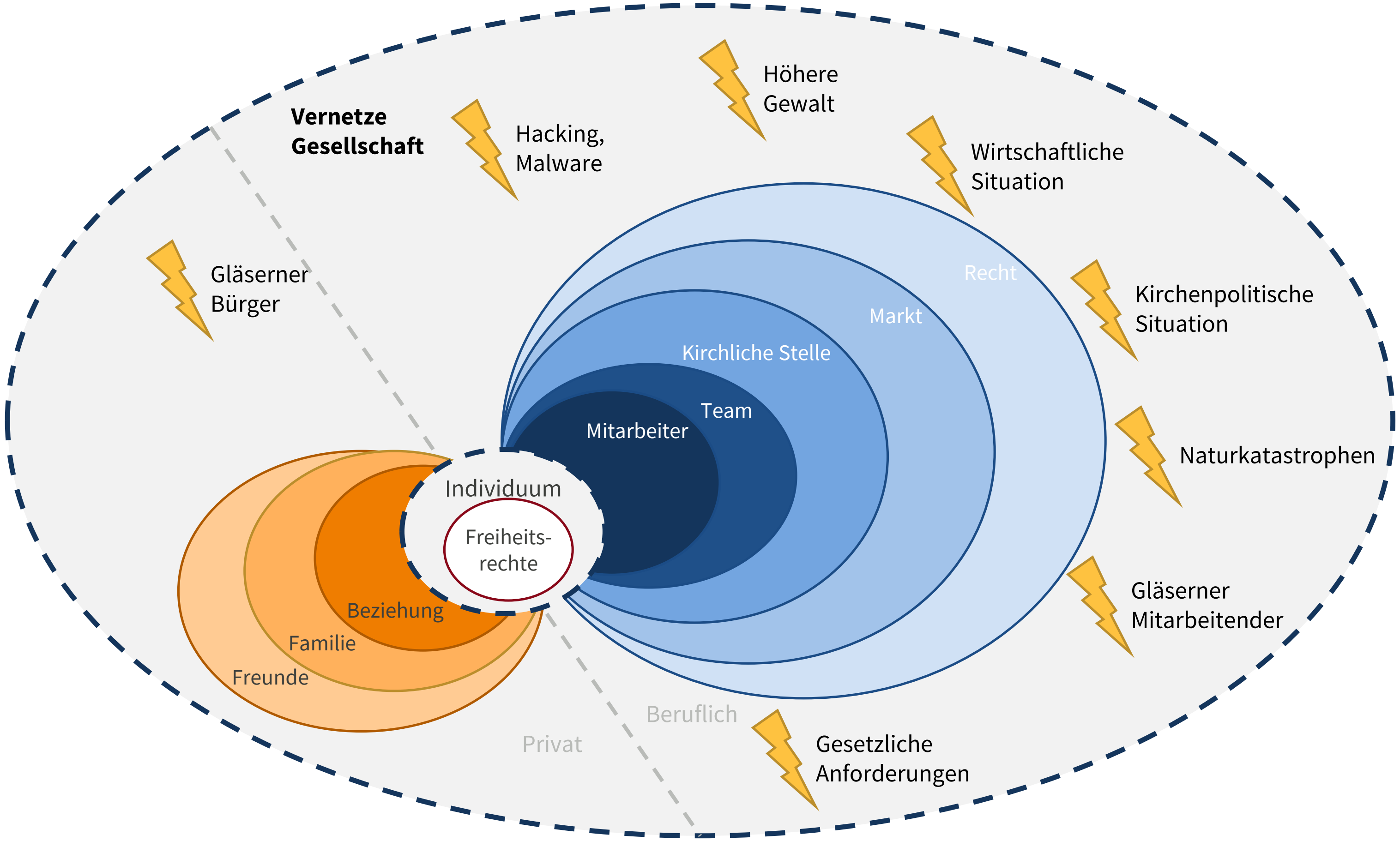
Evangelische Kirche in Deutschland

DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Anforderungen an die TOMs



Risikobetrachtung



Stand der Technik

- Technik, die sich in der Praxis bewährt hat und ein insofern anerkanntes Sicherheitsniveau bietet.
- Es muss sich um eine aktuelle Bewertung handeln:
  - Verpflichtung, den Stand der Technik aktiv zu verfolgen,
  - die eigenen TOMs daraufhin zu überprüfen
  - und sie nach Bedarf zu aktualisieren.
- „Stand der Technik“ bedeutet nicht, die jeweils neueste Technik oder Software einsetzen zu müssen.
- Es ist ein Kompromiss zwischen Aktualität und Verbreitung / Etablierung nötig.

Nachweisfähigkeit

- Maßstäbe eines internen Kontrollsystems (IKS) anwendbar
- „Test of Design“
  - Gibt es eine Vorgabe für die TOMs?
  - Ist sie dokumentiert?
  - Sind die Mitarbeitenden informiert und geschult?
  - Gibt es eine Kontrolle?
- „Test of Effectiveness“
  - Werden die TOMs umgesetzt?
  - Funktioniert die Kontrolle?
  - Ist die Umsetzung durch eine (der Grundgesamtheit der Geschäftsvorgänge angemessene) Stichprobe nachgewiesen?

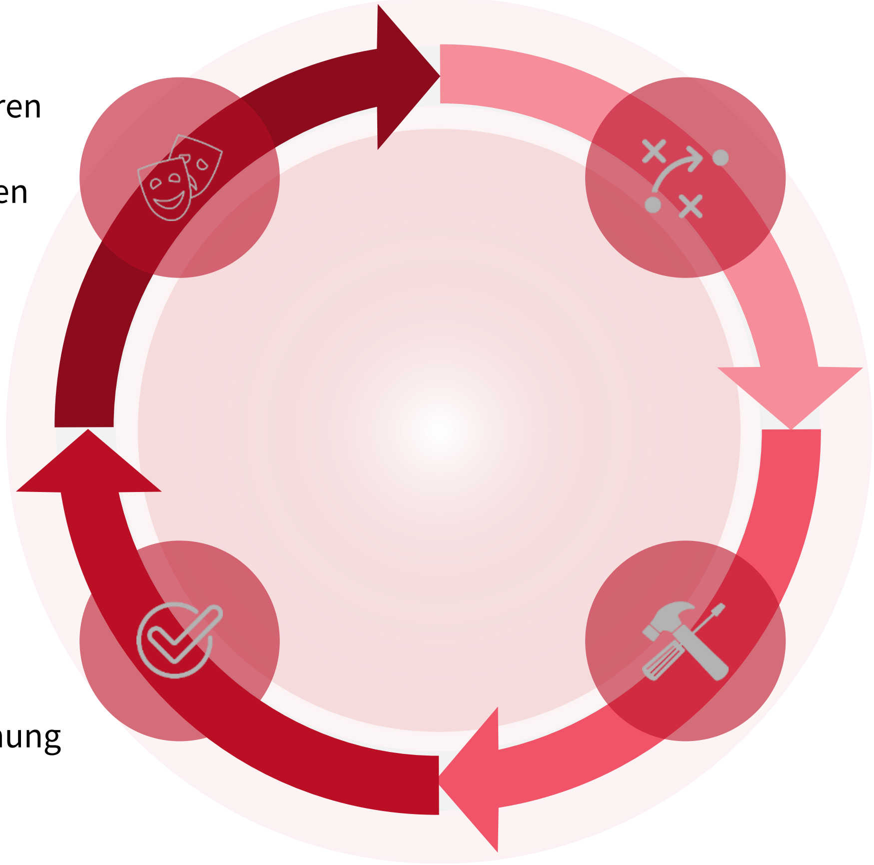
Regelmäßige Prüfung und Aktualisierung

- TOMs müssen nach Bedarf überprüft und aktualisiert werden.
- Verfahren ist vorzusehen, das die Maßnahmen, die die Sicherheit der Verarbeitung gewährleisten sollen, regelmäßig überprüft, bewertet und evaluiert (§ 5 Abs. 2 i.V.m. § 27 Abs. 1 DSG-EKD).

PDCA-Zyklus

Act

- Ggf. Aufsichtsbehörde konsultieren
- Verarbeitung überprüfen
- Verbesserung der TOMs anstreben (Stand der Technik)



Plan

- Sensibilität der Daten bestimmen
- Art, Umfang, Umstände, Zweck einer konkreten Verarbeitung bestimmen
- Risikobeurteilung
- Maßnahmen für Verarbeitung festlegen incl. „Privacy by Design / Default“
- Kontrolldesign festlegen

Check

- Interne / externe Audits
- Wirksamkeit bewerten
- Abweichungen zu geplanter Eignung ermitteln

Do

- TOMs umsetzen
- Umsetzung dokumentieren
- Restrisikobetrachtung
- Kontrollen implementieren

Verhältnismäßigkeit, § 27 Abs. 3 DSG-EKD

(1) Geeignetheit

Das Mittel ist geeignet, wenn der gewünschte Erfolg zumindest gefördert werden kann (er muss nicht unbedingt erreicht werden).

(2) Erforderlichkeit

Von mehreren geeigneten und möglichen Maßnahmen ist diejenige zu wählen, die den Einzelnen am wenigsten beeinträchtigt.

(3) Angemessenheit

Das angestrebte Ziel und die dafür in Kauf genommene Belastung sollen in einem ausgewogenen Verhältnis zueinander stehen.