**Folgenabschätzung (Theorie)**

(nach Koreng/Lachmann, Formularhandbuch Datenschutzrecht, 2. Auflage)

**Zuständig für die Durchführung:** Verantwortliche bzw. der Betriebserlaubnisinhaber

**Hinzuziehung des Datenschutzbeauftragten der Apotheke erforderlich**

**Zeitpunkt:** vor Beginn der Verarbeitung

**1. Beschreibung**

Systematische Beschreibung der geplanten Verarbeitungsvorgänge

* Art, Umfang, Umstände und Zwecke der Verarbeitung
* Art der personenbezogenen Daten, Empfänger und Speicherfristen
* eingesetzte Datenträger, Wissensträger und/oder Trägermedien (Hardware, Software, Netzwerke, Personen, Papier etc.)
* Branche, Rolle des Verantwortlichen und Rolle des Betroffenen
* zusammenfassend: Alle datenschutzrelevanten Sachverhaltsmerkmale und die eingesetzte Technik müssen so konkret beschrieben werden, dass sich die Phasen der Bewertung und der Bewältigung anschließen können.
* Systematische Beschreibung der Zwecke der Verarbeitung, z. B. Abrechnung, Diebstahlsschutz, Aufklärung von Straftaten
* Systematische Beschreibung der von dem Verantwortlichen verfolgten berechtigten Interessen: rechtlicher, wirtschaftlicher, ideeller oder sonstiger Art (Überschneidungen mit der Beschreibung des Zwecks möglich).

**2. Bewertung**

Systematische Prüfung der geplanten Verarbeitungsvorgänge und Bewertung der Risiken:

* Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
* Berücksichtigung und Abwägung von Betroffenenrechten und Risiken für die Rechte und Freiheiten der Betroffenen zum verfolgten Zweck
* Zur Bewertung der einzelnen Faktoren (nach ISO 29134, Annex A):

*Bemessung der Schwere*

|  |  |
| --- | --- |
| maximal | möglicher Eintritt signifikanter, sogar irreversibler Konsequenzen, die nicht überwunden werden können (Vernichtung der wirtschaftlichen Existenz, Arbeitsunfähigkeit, dauerhafte physische oder psychische Konsequenzen, Tod) |
| wesentlich | möglicher Eintritt signifikanter Konsequenzen, die sich – wenn auch ggf. mit großen Anstrengungen – wieder überwinden lassen (Verlust der Kreditwürdigkeit, Verlust von Eigentum, gesundheitliche Verschlechterung) |
| begrenzt | möglicher Eintritt signifikanter Konsequenzen, die sich mit nur geringen Anstrengungen wieder überwinden lassen (Zusatzkosten, Stress, geringe physische Belastungen) |
| vernachlässigbar | Eintritt allenfalls bloßer Belästigungen, die sich ohne Probleme ertragen lassen (Ärgernisse, kurzer Zeitverlust etc.) |

*Bemessung der Eintrittswahrscheinlichkeit*

|  |  |
| --- | --- |
| maximal | Realisierung der Bedrohung erscheint aufgrund der gewählten Ressourcen sehr leicht möglich (z. B. Aufbewahrung im öffentlich zugänglichen Bereich) |
| wesentlich | Realisierung der Bedrohung erscheint aufgrund der gewählten Ressourcen möglich (z. B. Aufbewahrung im öffentlich zugänglichen Bereich mit leicht umgehbarer Zutrittskontrolle/-beschränkung) |
| begrenzt | Realisierung der Bedrohung erscheint aufgrund der gewählten Ressourcen schwer möglich (z. B. einfache Zugangssicherung) |
| vernachlässigbar | Realisierung der Bedrohung erscheint aufgrund der gewählten Ressourcen nicht möglich (z. B. doppelte Zugangssicherung) |

**3. Bewältigung der identifizierten Risiken**

* Welche Maßnahmen können getroffen werden, um den Schutz personenbezogener Daten sicherzustellen, Garantien, Sicherheitsvorkehrungen etc.?
* Wer ist wann für die Maßnahmen zuständig?
* Woran wird der Erfolg der Maßnahmen gemessen

| **Schutzziel** | **denkbare Schutzmaßnahme gegen Bedrohung** |
| --- | --- |
| Vertraulichkeit | * Rollen- und Rechtekonzept mit regelmäßiger Prüfung und beschränkten Admin-Rechten
* Beschränkung des User-eigenen Hardware- und Software-Einsatzes
* Mandantentrennung, Partitionierung
* Verschlüsselung
* Protokollierung, Log-Dateien aller Anfragen und Server-Aktivitäten
* –T und Privacy-Compliance‑Richtlinie/Einbeziehung in Code of Conduct: z.B. Sperrbildschirm bei Verlassen des Arbeitsplatzes aktivieren
* Schulungen
* Verpflichtungs- und Vertraulichkeitserklärungen, NDAs der involvierten Personen
* Risikohinweise, z.B. auf Social Engineering, neue Angriffsformen
* gut sichtbare Warnhinweise auf in Dokumenten oder Dateien enthaltene personenbezogene Daten, ggf. sogar besonderer Kategorie gem. Art. 9 DS-GVO
 |
| Integrität | * Hash-Werte
* Zugriffskontrollen
* elektronische Signaturen
* Schreibschutz
* Lösch- und Korrekturkonzept
* Auditierung
* Protokollierung, Log-Dateien aller Anfragen und Server-Aktivitäten
 |
| Verfügbarkeit | * Zugriffskontrollen
* Redundanz
* Virenscanner-Einsatz
* Firewalls
* Partitionierung
* angemessene Speichermedien und -Umstände (Schutz gegen Feuer, Korrosion etc.)
* Vermeidung von Speicher-/Server-Standort mit geographischen, tektonischen, aber auch rechtlichen Herausforderungen (letzteres z. B. bei plötzlichem Wegfall des angemessenen Schutzniveaus)
 |
| Nichtverkettbarkeit und Zweckbindung | * Schulungen
* Rollen- und Rechtekonzepte, u. a. Grenzen von Admin-Rechten
* Anonymisierung
* Pseudonymisierung
 |
| Transparenz | * Dokumentation
* Protokollierung, auch von Änderungen, z. B. der Konfiguration
 |
| Invervenierbarkeit | * Zugriff zur Ausübung von Betroffenenrechten, unmittelbar oder über geeignete Kontaktperson/Hotline/Helpdesk
 |