Erstellen und Pflegen des Verfahrensverzeichnisses

Internes Verfahrensverzeichnis (§ 3a KDO)

Bestandsaufnahme über die laufenden Verarbeitungen von personenbezogenen Daten im Rahmen von automatisierten Verfahren

Wichtigstes Instrument zur Überwachung der ordnungsgemäßen Anwendung der KDO sowie der bereichsspezifischen Gesetze und Verordnungen (quasi betriebsinterne Selbstkontrolle bzgl. des Umgangs mit pbD)

Gesetzeskonformes Datenschutzmanagement

Was ist ein automatisiertes Verfahren?

- die Verwendung personenbezogener Daten
  - Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, z.B.:

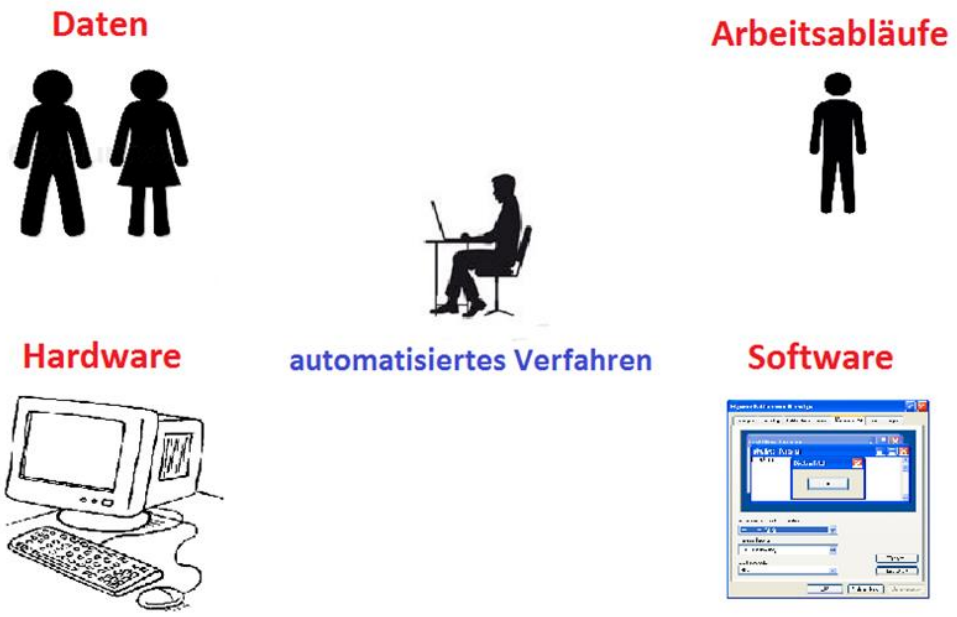
    Name, Alter, Familienstand, Geburtsdatum; Anschrift, Telefonnummer, E-Mail Adresse; Konto-, Kreditkartennummer, Kfz-Kennzeichen; Personalausweisnummer, Sozialversicherungsnummer; Vorstrafen; genetische Daten und Krankendaten; Werturteile wie zum Beispiel Zeugnisse
- zu einem bestimmten Zweck,
- mit Unterstützung von informationstechnischen Geräten (Hardware) und Computerprogrammen (Software),
- eingebunden in organisatorische Regeln (Aufbau- und Ablauforganisation).

→ Es bildet die Verwaltungsaufgaben, z.B. die Finanzbuchhaltung, Personalverwaltung usw., in einer datenverarbeitenden Stelle ab.

In der Regel lassen sich automatisierte Verfahren leicht identifizieren, beispielsweise bei der Verarbeitung von Beschäftigtendaten:

- **Zweck:** Verwaltung und Verarbeitung von Personaldaten zu Abrechnungszwecken
- **Hardware:** Server, Clients, Zugriff der Clients über das Netz
- **Software:** es wird ein Fachprogramm (z.B. Lexware) eingesetzt
- **Regeln:** nur autorisierte Personen (Mitarbeiterinnen und Mitarbeiter, in deren Zuständigkeit die Verarbeitung der Personaldaten liegt – Beschäftigte der Personalabteilung) dürfen die Daten einsehen bzw. verarbeiten.

Wichtig ist, dass nicht der Fehler gemacht wird, ein Programm mit einem automatisierten Verfahren gleichzusetzen. So sind Standardprogramme wie z.B. Microsoft Word keine automatisierten Verfahren im Sinne der Gesetzesdefinition, sondern lediglich die Software, die beispielsweise im Verfahren „Lohnabrechnung“ zur Verarbeitung von personenbezogenen Daten bei der Erstellung von Gehaltsabrechnungen eingesetzt wird.



- Ein internes Verfahrensverzeichnis als Bestandteil einer datenschutzkonformen Dokumentation der automatisierten Verfahren (Beschreibung des ordnungsgemäßen Einsatzes von Informationstechnik und der technischen und organisatorischen Maßnahmen).

- Den gesetzlich geforderten Inhalt gibt § 3a KDO vor.

- Das Verfahrensverzeichnis ist vorzuhalten, also zu erstellen und/oder aktuell zu halten
  - Auch wenn dem Datenschutzbeauftragte oder dem betrieblichen Ansprechpartner das Verzeichnis führt, bedeutet das im Umkehrschluss nicht, dass dieser für das Verfahrensverzeichnis alle notwendigen Informationen selber erhebt. Dieses Fachwissen liegt in den entsprechenden Fachabteilungen und sollte auch dort (in Zusammenarbeit) abgerufen werden

Transparenz der internen Datenverarbeitung

Bezeichnung des Verfahrens:

Lohn- und Gehaltszahlungen an die Beschäftigten

1. Name und Anschrift der verantwortlichen Stelle

   Muster gGmbH, Musterstraße 0, 00000 Musterstadt

2. Vertretung der verantwortlichen Stelle

   a) Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung der Stelle berufene Leiter

   b) Leitung der Datenverarbeitung (im konkreten Fall)

   Herr/Frau Mustermann (= Leitung Personalabteilung)

3. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung

   Ermittlung und Auszahlung von Lohn und Gehalt

4. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien

a) *Beschreibung der betroffenen Personengruppen*

Voll- und Teilzeitbeschäftigte, Leiharbeitnehmer, Praktikanten, Ferienarbeiter, Werksstudenten

b) *Beschreibung der Daten/Datenkategorien*

- *Name, Geburtsdatum, Nettolohn, Bruttolohn, Steuerklasse, Bankverbindung, Sozialversicherungsbeiträge, Krankenkasse, Konfession, Kirchensteuerbeitrag, Jahresnetto, Jahresbrutto, Stundenlohn, Überstunden, Zulagen, Sozialversicherungsdaten, Krankheitstage, Abwesenheit, Urlaubstage, Kinderfreibeträge*
- *Besonders sensible Daten (gem. § 2 Abs. 10 KDO) zu: Gesundheit*

5. Empfänger oder Kategorien von Empfängern, denen die Daten (ggf.) mitgeteilt werden
   - *Personalabteilung (intern)*
   - *Lohnbuchhaltung (intern)*
   - *Geschäftsführung (intern)*
   - *Fachvorgesetzte (intern)*
   - *Finanzamt (extern)*
   - *Buchhaltung/Controlling (intern)*
   - *Sozialversicherungsträger (extern)*
   - *Steuerberater (extern)*

6. Regelfristen für die Löschung der Daten
   - *10 Jahre bei Lohn- und Gehaltsdaten, Abrechnungsdaten, Bankdaten, Lohnsteuerdaten*
   - *6 Jahre bei Sozialversicherungsdaten/ Beitragsdaten*
7. Geplante Datenübermittlung ins Ausland
   - *geplant ja/ nein*
   - *Name des Drittstaates*
   - *Kategorie der Daten*
   - *Kategorien von Empfängern*
8. Allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 6 KDO zur Gewährleistung der Sicherheit der Bearbeitung angemessen sind
   - **Zutrittskontrolle**

     -> Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren

     (z. B.: abschließbare Bürotür, Chipkartensystem, geregelte Schlüsselverwaltung, Gebäudeüberwachung/Wachdienst)

- **Zugangskontrolle**

  -> Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

  (z.B.: Passwortregeln, Regelungen bei fehlgeschlagenen Anmeldeversuchen, automatische Bildschirmsperre, eindeutige Zuordnung von Benutzerkonten zu Benutzern)

- **Zugriffskontrolle**

  -> Gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

  (z.B. Restriktives Berechtigungskonzept, Netzlaufwerke mit Zugriff nur für berechtigte Benutzer/Benutzergruppen, Virenschutzkonzept)

- **Weitergabekontrolle**

  -> Gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

  (z.B.: Absicherung der Übermittlung durch Verschlüsselungsverfahren; Abgesicherter physikalischer Datenträgertransport, Vernichtung von Datenträgern)

- **Eingabekontrolle**

  -> Gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

  (z.B.: Protokollierung der Datenverarbeitung; Regelungen über die Löschung von Protokolldaten)

- **Auftragskontrolle**

  -> Gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

  (z.B.: sofern Dienstleister potentiell die Möglichkeit des Zugriffs auf pbD Daten haben: sichere Fernwartung und adäquate Vereinbarungen zur Auftragsdatenvereinbarung nach § 8 KDO)

- **Verfügbarkeitskontrolle**

  -> Gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

  (z.B.: Redundante Systeme, Datensicherung und Notfallkonzept, Archivierung)

- **Trennungsgebot**

  -> Gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

  (z.B.: Mandantenfähigkeit des Systems, keine Tests mit Originaldaten – vielmehr Test- und Produktivsystem getrennt halten)

9. Zugriffsberechtigte Personen
   - *Sachbearbeiter der Abteilung Rechnungswesen, die Buchungen durchführen*
   - *Vorgesetzte,*
   - *Geschäftsführung*
   - *jeweiliges Zugriffsrecht (wer kann die pbD lesen, verändern, löschen)*

Hinweise:

- Betrachten Sie während der Erstellung des Verfahrensverzeichnisses dieses immer aus der Sicht eines Abfragenden bestellten Datenschutzbeauftragten bzw. des Diözesandatenschutzbeauftragten der katholischen Kirche.
- Würden Sie die Beschreibungen zu den acht geforderten Punkten verstehen?
- Wären die Angaben für Sie ausreichend? Könnten Sie anhand dieser Informationen zur Einhaltung der Datensicherheit getroffenen Maßnahmen nachvollziehen ob Ihre Daten sicher verarbeitet werden?
- Vielleicht können Sie auch eine Kollegin oder einen Kollegen aus einem anderen Fachbereich dieses Verfahrensverzeichnis zu lesen geben; ergeben sich bei ihr oder bei ihm noch Fragen, dann sollten Sie die entsprechende Beschreibung optimieren.
- Denken Sie daran, dass Sie im Verfahrensverzeichnis ein automatisiertes Verfahren, d.h. eine Verwaltungsaufgabe (Geschäftsprozess), beschreiben und keine Software.
- Benennen Sie das Verfahren demnach so, dass Sie anhand des Namens nachvollziehen können, zu welchem Zweck die Daten verarbeitet werden, z.B. Lohn- und Gehaltsabrechnung, usw.

Vielen Dank für Ihre Aufmerksamkeit

Rechtsanwaltskanzlei Costard

Kanzlei für IT-Recht & Datenschutz

Bayreuther Straße 11

90409 Nürnberg

Tel : 0911/790 30 34

E-Mail: costard@it-rechtsberater.de