Praxisorientierter Beitrag für das

G-Forum 2020

Das 100%-Problem im Datenschutz

1 Ausgangssituation

Verschiedene Datenschutzgesetze verlangen, dass Unternehmen detaillierte Informationen über Praktiken der Datenerhebung, Datenverarbeitung, Weitergabe und Speicherung dokumentieren sowie an die betroffenen Personen kommunizieren. Im Falle der europäischen Datenschutz-Grundverordnung (DSGVO) müssen alle Verarbeitungsprozesse, die personenbezogene Daten betreffen, vollständig und aktuell in einem Verzeichnis der Verarbeitungsaktivitäten (VVT) dokumentiert werden.

In jedem Fall müssen die Unternehmen Transparenz hinsichtlich erhobenen und verarbeiteten Daten, der Verarbeitungsverfahren und –systeme sowie der internen und externen Datenströme herstellen und aufrechterhalten. Die Betroffenen müssen vor der Verarbeitung (gem. DSGVO) oder auf Anfrage (gem. verschiedener US Privacy Bills) über den Umfang und die Zwecke der Verarbeitung informiert werden.

Alle relevanten Verarbeitungsprozesse, inklusive der verarbeiteten Datenarten und Zwecke sind im VVT zu dokumentieren. Das Verzeichnis kann jederzeit von den Datenschutzbehörden angefordert und geprüft werden. Die Nachweispflicht liegt bei den Unternehmen.

Insbesondere in größeren, international agierenden Unternehmen sind die jeweiligen Entitäten in der Pflicht, Transparenz zu schaffen und Dokumentationsanforderungen umzusetzen. In der Praxis werden Dokumentations- und Aktualisierungsanforderungen auf Bereichs- oder Abteilungsebene heruntergebrochen. Es werden Rollen wie Prozess- und Dateneigner definiert, die für die Einhaltung der gesetzlichen Vorgaben hinsichtlich der Verarbeitungsprozesse im jeweiligen Verantwortungsbereich zuständig sind.

Die Erfassung und Aktualisierung von Verarbeitungsprozessen werden häufig abteilungsintern und somit dezentral umgesetzt. Unterstützt werden die Fachbereiche von eingesetzten Datenschutzbeauftragten oder Datenschutzkoordinatoren. Die Ergebnisse der dezentralen Erfassung oder Aktualisierung fließen schließlich in ein zentrales Verarbeitungsverzeichnis ein

2 Problemstellung

Verarbeitungsprozesse sind vielfältig, dynamisch und im ständigen Wandel. Um Aktualität sicherstellen zu können, sind laufende Anpassungen notwendig. Einige Verfahren sind über einen längeren Zeitraum hinweg beständig, andere ändern sich häufig. Ein regelmäßiger Turnus zur Prüfung der Aktualität ist somit nur bedingt geeignet.

Verarbeitungszwecke und –Techniken sind ebenfalls dynamisch. Insbesondere bei der (Weiter-) Entwicklung digitaler Produkte und dem steigenden Einsatz neuer Technologien in der Datenverarbeitung, steigen die Verarbeitungsmöglichkeiten. Den Betroffenen vorab, vollständig über Umfang und Zwecke zu informieren steht einer stetigen Entwicklung in der Verarbeitung entgegen.

Zudem wird Verarbeitung personenbezogener Daten wird nicht zwangsläufig als solche identifiziert. Dies ist der Fall, wenn Datenkategorien verarbeitet werden, die ohne konkrete Kenntnisse nicht als personenbezogene oder personenbeziehbare Daten erkannt werden (z.B. Fahrzeug-Identifizierungsnummer). Weiterhin besteht eine Herausforderung in der Identifikation von personenbezogenen Daten, die sich aus einer Kombination verschiedener, isoliert betrachtet unkritischer Daten, ergeben kann.

Darüber hinaus ist die Vollständigkeit (100%) des VVTs zumeist unbekannt. Es ist nicht möglich eine „Soll-Situation“ zu definieren, wenn der betreffenden Organisation, die Gesamtheit der existenten Datenverarbeitungsprozesse nicht bekannt ist. Somit kann weder die vollständige Umsetzung, noch der Erfüllungsgrad der Anforderungen umfassend geprüft werden. Insbesondere gilt dies für größere Unternehmen mit verschiedenen Entitäten und Geschäftsbereichen.

<u>Grundlegende Fragestellungen in der Organisation:</u>

- Was sind personenbezogene Daten und in welchen Prozessen werden diese verarbeitet?
- Auf welchen Rechtsgrundlagen der Verarbeitung basieren die Verarbeitungsprozesse?
- Welche Verarbeitungszwecke liegen vor und wann entfallen diese bzw. wann muss gelöscht werden?
- Für welche personenbezogenen Daten besteht eine Aufbewahrungspflicht und wie lange müssen die betreffenden Daten gespeichert werden?
- Kennt jeder Mitarbeiter die rechtlichen Vorgaben und die operativen Auswirkungen sowie Handlungsbedarfe
- Ist jeder Mitarbeiter in der Organisation in der Lage, die relevanten Prozesse zu identifizieren, dokumentieren und Handlungsbedarfe abzuleiten? (inkl. Betriebsarzt, Empfang, Personalwesen, etc.)
- Sind Verantwortlichkeiten (ins. DPO, CISO etc.) und der Verantwortungsübergang klar geregelt?

- Kann die Vorlagefähigkeit unter Einhaltung der Anforderungen gemäß Art. 30 DSGVO, gewährleistet und aufrechten werden?

3 Auswirkungen in der Praxis

Das Verzeichnis der Verarbeitungstätigkeiten wird häufig mit großem manuellen Aufwand erstellt. Dezentral erhobene und beschriebene Verfahren werden in einer zentralen Datei dokumentiert. Es gibt Bestrebungen, dieses Vorgehen zentral zu steuern, zu unterstützen und nachzuverfolgen. Es bestehen offizielle sowie häufig unternehmensinterne Leitlinien und beschriebene Dokumentationsanforderungen. Teilweise kommen unterstützend auch Tools und Systeme zum Einsatz (z.B. Privacy Management Tools und Software). Die Nachverfolgung und Prüfung erfolgt nachgelagert ohne dabei den Soll-Zustand hinsichtlich Vollständigkeit und Aktualität zu kennen.

Prüfungshandlungen können Abweichungen identifizieren, allerdings:

- werden nur Abweichungen identifiziert, die im Prüfungsprogramm explizit enthalten sind. Ohne Kenntnis über den Soll-Zustand (die 100%), ist ein Soll/Ist Abgleich nicht möglich
- spiegeln die Ergebnisse lediglich den Stand des Prüfungszeitpunktes wider. Durch Prüfungen im üblichen Audit-Rhythmus können Risiken und Handlungsbedarfe weder zeitnah noch lückenlos identifiziert werden
- ist das Audit nachgelagert und ersetzt nicht die von der Unternehmensleitung eingerichteten Risikokontrollen zur Einhaltung gesetzlicher Vorschriften.
- ist eine manuelle Prüfung von verschiedenartigen Prozessen mit verschiedenen Merkmalen von bis zu mehreren tausend Verarbeitungsprozessen sehr aufwändig
- erfordert jede neue Entwicklung in der Verarbeitung eine Prüfung und ggf. erneute Umsetzung von Informationspflichten und Anpassung der Prozessdokumentation
- stehen heterogene Prozesse und vielfältige Systemlandschaften einem zentralen, einheitlichen Prüfprogramm entgegen
- können Kompetenzen, Kapazitäten und Prioritäten innerhalb einer Organisation stark voneinander abweichen

4 Implikationen für Forschung und Praxis

Um trotz der steigenden Anzahl an Verarbeitungsprozessen und des wachsenden Umfangs verarbeiteter Daten, Transparenz herzustellen und dauerhaft zu gewährleisten zu können, wächst der Bedarf an neuen Technologien für ein effektives Datenschutzmanagement.

Es bedarf Managementkontrollen sowie geeignete Instrumente zur Risikokontrolle und Überwachung hinsichtlich der Einhaltung von Vorschriften (1st & 2nd line of defense). Systemische Unterstützung bei der Erhebung, Dokumentation, Aktualisierung sowie Prüfung erforderlich, um die enormen manuellen Aufwände zu reduzieren und einen höheren Erfüllungsgrad erreichen zu können

Dabei rücken neue Tools und Technologien wie Data -und Process Mining, die es ermöglichen Verarbeitungsprozesse und Datenströme zu visualisieren, weiter in den Fokus. Der Einsatz von künstlicher Intelligenz, Algorithmen und Systemen zur Abbildung und laufenden Kontrolle von Daten im Unternehmen kann sowohl die Konformität als auch die Effizienz erheblich unterstützen. Abweichungen und Veränderungen innerhalb von Datenverarbeitungsprozessen können erkannte und Risiken sowie Handlungsbedarfe effizient abgeleitet werden.

Künstliche Intelligenz kann zur Erkennung von Verarbeitungsprozessen auf Basis verschiedener Merkmale eingesetzt werden. In weiteren Ausbaustufen können Möglichkeiten zur laufenden Identifikation von Veränderungen in den Verarbeitungsprozessen, zur Prüfung der Umsetzung fachlicher Löschkonzepte anhand verschiedener Merkmale, zur Identifikation von Verarbeitungszwecken, den Abgleich mit den umgesetzten Informationspflichten sowie Rechtsgrundlage der Verarbeitung, entwickelt werden.

Ein globaler, industrieübergreifender Einsatz ist möglich. Die Durchführung von Prüfungshandlungen als auch die unternehmensinterne Umsetzung in Form eines Datenschutzmanagement-Systems, zur Reduktion und Kontrolle von Compliance-Risiken im Unternehmen wird angestrebt. Um der beschriebenen Problemstellung angemessen zu begegnen, bestehen Forschungsbedarfe und vielfältige Forschungsansätze, insbesondere bei der Entwicklung geeigneter technischer Lösungen.