

Datenschutz im digitalen Alltag

Daniela Tschol, Markus Güdel

Die modernen Hilfsmittel der Informatik bieten umfassende Funktionen und gewähren so beispielsweise die Möglichkeit für das einfache Sammeln, Aufbereiten sowie das Verknüpfen, Kopieren und Weitergeben von Personendaten. Dies ruft im Kontext des Datenschutzes nach mehr Sicherheit und Wissen im Umgang mit der digitalen Bearbeitung von Daten.

Datenschutz bedeutet Compliance

In rechtlicher Hinsicht verstehen wir unter Datenschutz den Schutz von Daten mit einer Aussage über eine bestimmte oder bestimmbare Person (Art. 3 lit. a Datenschutzgesetz des Bundes, kurz DSGVO).

Firmeninterne Datenbearbeitungsprozesse bedürfen einer vorgängigen datenschutzrechtlichen Überprüfung, damit sie rechtmässig in Softwarelösungen umgesetzt werden können.

Den Normen des Datenschutzes unterliegt jeder, der Daten bearbeitet. Unter Bearbeiten versteht man jeden Umgang mit Daten, wie das Erwerben, Kopieren, Archivieren usw., aber auch das blosses Aufbewahren.

Bezogen auf Unternehmungen kann gesagt werden, dass die Einhaltung der Datenschutzvorschriften in den Verantwortungsbereich des Managements gehört. Datenschutz ist somit Chefsache. Datenschutz ist sowohl im Innenverhältnis der Unternehmung ein Thema, beispielsweise Daten betreffend Mitarbeitende oder finanzwirtschaftliche Daten, als auch im Aussenverhältnis von Relevanz, d.h. was Daten von Kunden, Lieferanten, Konkurrenten usw. anbelangt.

Rechtmässige Datenbearbeitung

Es gelten folgende Grundsätze zur allgemeinen rechtmässigen Datenbearbeitung:

- Eine Datenbearbeitung muss immer zweckmässig sein. Personendaten dürfen folglich nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.
- Die Zweckmässigkeit der Datenbearbeitung ist im Zusammenhang mit der Verhältnismässigkeit zu beurteilen. Eine Datenbearbeitung muss verhältnismässig zum angegebenen Zweck sein. Das heisst, sie muss ge-





eignet und notwendig sein, um den angestrebten Zweck zu erreichen. Zudem dürfen nur so viele Personen wie unbedingt notwendig Zugriff auf die Daten haben. Ein unbeschränkter Zugriff auf die Daten ist nicht zweck- und verhältnismässig. Es stellt sich deshalb bei jeder Bearbeitung die Frage: «Wer macht was warum wie lange?»

- Als dritter Grundsatz ist die Richtigkeit von Daten zu überprüfen. Die Verantwortlichen müssen alle angemessenen Massnahmen treffen, damit die Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. Jede betroffene Person hat ein Auskunftsrecht und kann die Berichtigung ihrer Daten verlangen.
- Sicherheit – schlussendlich müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Dazu gehören insbesondere die Gewährleistung der Vertraulichkeit, der

Verfügbarkeit und der Integrität der Daten.

Datenschutzanforderungen an IT-Prozesse

Auch technische Hilfsmittel einer Unternehmung müssen, wenn mit ihrer Hilfe entsprechende Daten bearbeitet werden, zwingend die Vorschriften des DSGVO bezüglich Datenbearbeitung und Datensicherheit erfüllen.

Damit eine Software die firmeninternen Bearbeitungsprozesse effizient und datenschutzkonform unterstützen kann, müssen in einem ersten Schritt die Firmenprozesse korrekt eruiert werden. Die Unternehmung muss sich im Klaren sein,

- welche Daten wie beschafft werden,
- von wem wie lange und
- in welchem Prozess bearbeitet und
- wie die Daten anschliessend weitergegeben werden.

In einem zweiten Schritt überprüft die Unternehmung (mit Vorteil in Zusammenarbeit mit einem unabhängigen, fachkundigen Berater) die prozess-

bezogenen notwendigen Datenschutz-Compliance-Anforderungen, woraus die konkreten datenschutzrechtlichen Anforderungen an die Bearbeitung von Daten abgeleitet werden können. Diese Prozesse können dann entsprechend in der Software implementiert und umgesetzt werden.

Kurz gesagt: Eine Unternehmung muss sich im Klaren darüber sein, welchen Compliance-Anforderungen die Software gerecht werden muss.

Umsetzung bei der digitalen Bearbeitung

Es müssen zahlreiche Bedingungen erfüllt sein, um Daten rechtmässig in einer Software bearbeiten zu dürfen:

- Die Erfassung einer Information in ein Datenverarbeitungssystem darf nur zweckmässig erfolgen, also nur gestützt auf die bei der Erhebung der Information angegebenen Gründe. Ist die Information einmal im System gespeichert, ist darauf zu achten, dass jede weitere Verarbeitung, Verknüpfung oder

- Zugänglichmachung der Information wiederum dieser Anforderung gerecht werden muss.
- Verhältnismässig: Im IT-Bereich werden den Usern je nach Bearbeitungsaufgabe verschiedene Berechtigungen zugewiesen. Inhalt und Umfang dieser Berechtigungen orientieren sich an einem internen Zugriffs- und Berechtigungskonzept, welches auf den gesetzlichen Grundlagen basiert.
 - Die Institution, welche IT-basierende Datenverarbeitungen nutzt, muss sicherstellen, dass die User ihre Eingaben entsprechend überprüfen, insbesondere dass die von ihnen bearbeiteten Daten richtig und vollständig sind. Im Bereich der Datenbearbeitung geschieht dies grundsätzlich mittels Plausibilitätsprüfungen. Zu diesem Zweck wird automatisch eine Vielzahl von Plausibilitätsregeln überprüft, sobald eine Dateneingabe stattfindet. Je nach Anwendungsbereich können einer Software weitere, fallspezifische Regeln hinzugefügt werden.
 - Die IT-Systeme müssen gegen folgende Risiken geschützt werden
 - unbefugte oder zufällige Vernichtung
 - zufälliger Verlust
 - technischer Fehler
 - Fälschung, Diebstahl oder widerrechtliche Verwendung
 - unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen
 - Schlussendlich muss die Einhaltung der korrekten, datenschutzkonformen Bearbeitung auch überwacht werden. Durch Aufzeichnungen und insbesondere die Zusammenstellung der Daten in Reports können Persönlichkeitsprofile über Mitarbeitende entstehen. Die Erstellung von Reports stellt deshalb ebenfalls eine Datenbearbeitung dar, welche den Anforderungen bezüglich Zweck, Verhältnismässigkeit, Richtigkeit und Sicherheit genügen muss.
- ## Zusammenfassung
- Zusammengefasst sind folgende zentrale Punkte beim Einsatz von IT-Lösungen zur Bearbeitung von Daten zu beachten:
- Vorab ist eine Überprüfung des Businessprozesses der Unternehmung durchzuführen. Dieser Prozess wird abgebildet und wenn nötig optimiert.
 - Anschliessend erfolgt eine Überprüfung dieser Prozessabbildung auf Datenschutzkonformität, idealerweise durch einen unabhängigen, fachspezifischen Dritten.
 - Erst danach erfolgt die Erstellung einer sauberen Abbildung dieses Prozesses in der Software.
 - Eine jährliche Überprüfung des Bearbeitungszweckes ist unumgänglich, um die Datenschutzkonformität einzuhalten.
 - Die Monitoringfunktion ist für die Überprüfung der Richtigkeit und Sicherheit des Systems zuständig. Eine entsprechende Information beziehungsweise Genehmigung der Mitarbeitenden ist für die Legitimation der Überwachung zwingend notwendig. ■