Name: 17.06.20

IB No.:

Klasse:

Datensicherheitskonzept

Sinn und Zweck:

Das **Bundesdatenschutzgesetz** regelt wie mit Daten, insbesondere personenbezogenen Daten, bei maschineller Verarbeitung umgegangen wird und welche Voraussetzungen ein Betrieb erfüllen muss. Eine Anlage zu dem §9 regelt die für die Informationsverarbeitung wichtigen Bestimmungen.

Anlage
(zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu 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 (Zugriffskontrolle),
4. zu 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, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Betrachten wir die einzelnen Punkte genauer:

Nr. 1 - Zutrittskontrolle

Die Zutrittskontrolle verlangt Maßnahmen, die Unbefugten den körperlichen Zutritt zu Datenverarbeitungsanlagen, mit den personenbezogene Daten verarbeitet werden, verwehren. Es soll also verhindert werden, dass unbefugte Personen überhaupt die Möglichkeit des Zugriffs auf Datenverarbeitungsanlagen haben. Die Zutrittskontrolle soll aber nicht nur einen unbefugten Zugriff auf Daten, sondern auch eine Zerstörung von EDV-Anlagen verhindern.

Die Zutrittsberechtigungen sind daher immer genau festzulegen und zu dokumentieren. Dies gilt insbesondere auch für unternehmensfremde Personen wie Wartungstechniker (denen immer Begleitpersonen an die Seite gestellt werden sollten) oder das Reinigungspersonal. Zur Zutrittskontrolle gehören aber auch alle Maßnahmen, die ein gewaltsames Eindringen verhindern.

Eine effektive Zutrittskontrolle ist in der Regel nur durch eine Kombination von verschiedenen ineinandergreifenden Maßnahmen möglich. Solche Maßnahmen könnten unter anderen sein:

- Fenstervergitterungen oder Sicherheitsfolien
- Alarmanlagen
- Videoüberwachung (außen und innen)
- Einrichtung verschiedener Sicherheitszonen mit verschiedenen Zutrittsberechtigungen
- Restriktive Schlüsselregelungen
- Mitarbeiterausweise und das sichtbar Tragen derselben
- Physische Gerätesicherungen (Kensington-Schlösser)
- Organisatorische Trennung von zugriffsberechtigten Personen
- Besucheraufenthalte nur mit Begleitpersonen
- Sichtkontrollen und Gästelisten am Empfang/Pförtner

Nr. 2 - Zugangskontrolle

In Abgrenzung zur „räumlichen“ Zutrittskontrolle sollen Maßnahmen der Zugangskontrolle die Benutzung von Datenverarbeitungsanlagen durch unbefugte Personen verhindern. Es muss hier eine Identifikation der Nutzer und Prüfung der Berechtigungen erfolgen um eine unzulässige Kenntnisnahme oder gar eine Änderung von personenbezogenen Daten zu verhindern.

Mögliche Maßnahmen der Zugangskontrolle sind beispielsweise:

- Anlegung einer zentralen Benutzerverwaltung
- Einrichtung verschiedener Berechtigungsstufen und Zuteilung derselben auf die Nutzer

- Einrichtung von Verfahren zur Identifizierung des Nutzers
- Zentral überwachte Passwortvergabe mit entsprechenden Anforderungen an die Komplexität des Passwortes und die Häufigkeit der Änderung desselben
- Aufzeichnung aller Zugriffsversuche
- Sperren von Arbeitsplätzen und/oder Benutzernamen bei fehlerhaften Zugriffsversuchen
- Verwendung eines Virtual Private Networks (VPN)
- Verschlüsselung von Daten und Festplatten

Für die Zugangskontrolle gibt es auch Empfehlungen des Bundesbeauftragten für den Datenschutz welche auf der Internetseite http://www.bfdi.bund.de abrufbar sind.

Nr. 3 - Zugriffskontrolle

Mitarbeiter und Dritte mit entsprechenden Berechtigungen sollen natürlich nur auf Daten zugreifen können, die für Ihre Arbeit relevant und erforderlich sind. Bei der Zugriffskontrolle geht es daher darum die berechtigten Zugriffe auf Daten insoweit zu beschränken als es für die zugreifenden Personen möglich und nötig ist.

Die verschiedenen Berechtigung können dabei den Zugriff auf bestimmt Teile des Netzwerkes, bestimmte Programme und/oder bestimmte Bearbeitungsrechte (Leserechte, Druckrechte, Veränderungsrechte) regeln. Darüber hinaus kann es sich auch hier anbieten berechtigte Zugriffe zu protokollieren um später nachvollziehen zu können, wer wann auf welche Daten zugegriffen und diese eventuell verändert hat.

Maßnahmen der Zugriffskontrolle können sein:

- Einrichtung verschiedener Berechtigungsstufen und Zuteilung derselben auf die Nutzer
- Zentrale Rechteverwaltung durch Administrator
- Einrichtung und Auswertung von Zugriffsprotokollen
- Lagerung von Datenträgern in speziellen Räumen mit Zutrittsbeschränkungen
- Festlegung von Zugriffsrechten auf Datenträger
- Vernichtung von Datenträgern nach DIN 32757#
- Vernichtung von Ausdrucken durch Aktenvernichter
- Protokollierung der Vernichtung von Datenträgern
- Verschlüsselung von Festplatten

Nr. 4 - Weitergabekontrolle

Die in Nummer 4 der Anlage geregelte Weitergabekontrolle betrifft im Grunde zwei verschiedene Szenarien. Zum einen wird auf die Sicherung der Übertragungswege von personenbezogenen Daten gleich ob per Datenträger oder elektronisch abgezielt. Zum anderen betrifft die Weitergabekontrolle auch Revisionsfähigkeit von Datenübermittlungsvorgängen an unternehmensfremde Dritte.
Hinsichtlich des ersten Szenarios müssen Unternehmen Maßnahmen treffen um zu verhindern, dass Unbefugte während eines Übertragungsvorgangs Zugriff – gleich

welcher Art – auf personenbezogene Daten haben. Umfasst werden dabei aber nicht nur die elektronische Übermittlung, sondern beispielsweise auch die Verbringung eines Back-Up-Datenträgers in einen Archivraum. In jedem Fall der Datenübermittlung sind entsprechende Sicherheitsmaßnahmen zu treffen. Dies gilt auch für die Auftragsdatenverarbeitung und dort die Weitergabe von Daten an den Auftragnehmer.

Das zweite Szenario verlangt eine „vorbeugende“ Dokumentation darüber, welche Empfänger personenbezogene Daten durch Datenübertragung erhalten sollen. Die Regelung verlangt dabei keine ständige Protokollierung sämtlicher Datenübertragungen, sondern vielmehr soll nur die vorgesehene Übermittlung dokumentiert werden. Für diese Dokumentation müssen alle Übermittlungsadressaten inklusive der an sie zu übermittelnden Datenmenge bezeichnet werden. Des Weiteren müssen die möglichen Übermittlungen in zeitlicher Hinsicht (Beginn und Ende der Übermittlung) überprüfbar sein. Die entsprechenden Dokumentationsunterlagen müssen auch für Dritte einsehbar und in einem entsprechend allgemein lesbaren Format vorhanden sein.

Folgende Maßnahmen sollen beispielhaft für eine Umsetzung der Weitergabekontrolle genannt werden:

- Verschlüsselung von Daten vor der Weitergabe
- Verschlüsselung von Datenträgern
- Wenn möglich Weitergabe von Daten in anonymisierter Form
- Benutzung sicherer Transportbehälter (Versiegelung)
- Identitätsüberprüfung beim Empfänger
- Dokumentation der Übermittlungsprogramme
- Revisionssichere aktuelle Übersicht

Nr. 5 - Eingabekontrolle

Wie bereits weiter oben erwähnt, macht es immer auch Sinn zu protokollieren, wer wann auf welche Daten zugreift, und was verändert wird. Die Maßnahmen zur Eingabekontrolle sollen genau das sicherstellen. Mit ihnen soll sich jederzeit ermitteln lassen, wer bestimmte Daten erstellt hat, was der Inhalt dieser Daten war und ist und wann die Erstellung bzw. Änderung vorgenommen wurde. So soll ermittelt werden können, wer für falsche oder unvollständige Daten verantwortlich zeichnet. Nicht gespeichert werden dürfen dabei aber die gelöschten oder veränderten Daten an sich. Es obliegt den Unternehmen wie die Identifizierung des „Datenurhebers“ umgesetzt wird. Es ist dabei nicht erforderlich, dass sich diese bereits direkt aus dem Datenverarbeitungssystem ergibt. Ausreichend ist beispielsweise auch eine Identifizierungsmöglichkeit über Eingangskontrollbücher oder Schichtpläne.

Zu beachten ist, dass mit der Anfertigung von Eingabeprotokollen eine neue Sammlung personenbezogener Daten entsteht, die als solche behandelt werden muss. Bei einer automatisierten Erstellung sollte daher darauf geachtet werden, dass sich einzelne Einträge auch nur automatisiert wieder ermitteln lassen.

Maßnahmen der Eingabekontrolle können unter anderem sein:

- Protokollierung der Nutzer, welche Eingaben tätigen
- Protokollierung aller Datenveränderungen
- Aufzeichnung von Protokollen direkt mit dem jeweiligen Datensatz
- Sicherung der Protokolldateien gegen unbefugte Nutzung und Veränderung

Der thüringische Datenschutzbeauftragte hat für Protokolldateien folgende allgemeine Hinweise veröffentlicht :

„Eine Erzeugung von Protokolldateien ist nur zulässig, wenn sie auch erforderlich sind, d. h. tatsächlich genutzt werden. Werden sie ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes der EDV-Anlage gespeichert, dürfen sie nur für diese Zwecke verwendet werden (§ 20 Abs. 4 ThürDSG). Werden Protokolldateien der genannten Art länger als drei Monate vorgehalten, sind sie in das Anlagen- und Verfahrensverzeichnis gem. § 10 Abs. 2 ThürDSG aufzunehmen und müssen darüber hinaus dem TLfD zum Datenschutzregister gem. § 3 Abs. 1 ThürDSRegVO gemeldet werden. Dies gilt nicht für Dateien, die vorübergehend und ausschließlich aus verarbeitungstechnischen Gründen erstellt und nach ihrer ordnungsgemäßen Nutzung automatisch gelöscht werden (§ 2 Abs. 2 ThürDSG).

Im Allgemeinen ist davon auszugehen, dass die Protokolldateien zur Verhaltens- und Leistungskontrolle geeignet sind. Es erscheint daher unerlässlich, den Personalrat oder Betriebsrat auf die Protokolldatei(en) hinzuweisen, damit dieser gegebenenfalls von seinen Mitbestimmungsrechten Gebrauch machen kann. Die zulässigen Auswertungen der Protokolldateien sowie die Art ihrer Nutzung sollten unter Beteiligung des internen Datenschutzbeauftragten und des Personalrates oder Betriebsrates festgelegt werden. Tatsächliche Auswertungen zu Zwecken der Datenschutzkontrolle oder der Kontrolle der IT-Sicherheit sollten durch den Datenschutzbeauftragten bzw. IT-Sicherheitsbeauftragten unter Beteiligung des Personalrates erfolgen.

Eine wahllose Registrierung aller Aktivitäten des Benutzers ist aus Sicht des Datenschutzes bedenklich. Zwar erfordert § 9 ThürDSG Maßnahmen, damit nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zur welcher Zeit von wem in das System eingegeben wurden. Der Angemessenheitsgrundsatz des § 9 gestattet es jedoch, dahingehende Registrierungen in Protokolldateien auf sensiblere Aktivitäten (Benutzung bestimmter Programme, Dateien, Datenfelder) zu begrenzen. Es sollten daher alle systemseitig vorhandenen Möglichkeiten - durch Einstellen von Parametern oder Setzen von "Schaltern" - genutzt werden, damit wirklich nur Aktivitäten mit erhöhtem Schutzbedarf registriert werden. So reicht es aus, wenn beispielsweise nicht jeder Zugriff auf eine Personaldatei registriert wird, sondern nur diejenigen, die besonders sensible Datenfelder oder Programme betreffen. Auch eine solche Protokolldatei darf nicht zur Verhaltens- und Leistungskontrolle genutzt werden. Protokolldateien müssen nach angemessener Zeit (automatisch) gelöscht werden; eine Speicherdauer von maximal einem Jahr ist im Allgemeinen als ausreichend anzusehen (siehe auch Nr. 2).“

Nr. 6 - Auftragskontrolle

In Ergänzung zu § 11 BDSG, welcher die rechtlichen Rahmenbedingungen für eine Auftragsdatenverarbeitung regelt, soll die Auftragskontrolle sicherstellen, dass sich der Auftragsdatenverarbeiter auch an die Weisungen des Auftraggebers hält und Datenverarbeitung nur innerhalb dieser Weisungen stattfindet. Denn allein die Weisungsgebundenheit führt dazu, dass eine Weitergabe von Daten an den Auftragnehmer nicht als Weitergabe an Dritte gewertet wird, welche zustimmungsbedürftig wäre.

Die Auftragskontrolle verlangt deshalb nach in Art und Umfang verhältnismäßigen Maßnahmen, welche sicherstellen, dass das Übermitteln, Speichern, Nutzen, Verändern und Löschen personenbezogener Daten nur nach Vorgabe des Auftraggebers beim Auftragnehmer erfolgen kann. Zum einen hat also der Auftragnehmer die Weisungen des Auftraggebers einzuhalten, zum anderen muss der Auftraggeber dafür Sorge tragen, dass seine Weisungen verständlich und umsetzbar sind und auch befolgt werden.

Die Weisungen können dabei in jeder Form erteilt werden, es empfiehlt sich jedoch eine Form zu wählen, die zum einen Irrtümer vermeidet und später ordentliche Nachweise ermöglicht. In der Praxis lassen sich diese Erfordernisse am besten über die Nutzung von Formularen (schriftlich oder elektronisch) bei der Auftragserteilung umsetzen. In den Weisungen sollte immer auch enthalten sein, welche Daten wie übermittelt werden sollen.

Erfolgte Maßnahmen sind sowohl vom Auftraggeber, als auch vom Auftragnehmer ständig auf ihre Umsetzung zu überprüfen und gegebenenfalls zu verbessern. Mögliche Maßnahmen wären zum Beispiel:

- Beachtung der erforderlichen Sorgfalt bei der Auswahl des Auftragnehmers
- Erteilung von Weisungen in schriftlicher oder elektronischer Form
- Schriftliche Bestätigung von mündlichen Weisungen
- Verwendung von Formularen
- Verschlüsselte Datenübergabe
- Abschluss einer Geheimhaltungsvereinbarung
- Regelung über Datenlöschung/-vernichtung bei Auftragsbeendigung
- Regelmäßige Kontrolle der Umsetzung
- Vertragliche Vereinbarung von Konventionalstrafen für Zuwiderhandlungen

Nr. 7 - Verfügbarkeitskontrolle

Durch Brand- und Wasserschäden, Blitzschlag oder Stromausfall oder aber Diebstahl und Sabotage können Datenbestände in Gefahr geraten. Dass in diesen Fällen kein Datenverlust eintritt soll die Verfügbarkeitskontrolle sicherstellen.

Der Schutz vor zufälliger Zerstörung kann hauptsächlich über die Einhaltung entsprechender Brandschutzvorschriften und durch zusätzliche Hardware zur unterbrechungsfreien Stromversorgung und Netzwerksicherheit sichergestellt werden. Mit den entsprechenden Vorkehrungen und Zusatzsoftware können EDV-Systeme

beispielsweise im Falle eines plötzlichen Stromausfalles noch so lange weiterbetrieben werden, bis ein kontrolliertes Abschalten möglich ist. Hierdurch können sowohl Datenverlust als auch Hardwareschäden vermieden werden.

Unter die Verfügbarkeitskontrolle fallen aber auch Maßnahmen zur Datensicherung, also die klassischen Backup- und Datenspiegelungslösungen. In welchen Intervallen solche Datensicherungen durchgeführt werden müssen, hängt immer von der Art der Daten, der Veränderungshäufigkeit und der Wichtigkeit der Daten für das Unternehmen ab. Für alle Datensicherungen gilt aber, dass auch die erstellte Sicherung vor Zerstörung und Diebstahl gesichert sein muss. Sicherungskopien dürfen daher nie im gleichen Gebäude oder Brandabschnitt wie das Datenverarbeitungssystem aufbewahrt werden. Vielmehr ist zu empfehlen, die Datensicherung entweder direkt auf einem Server an einem anderen Standort zu erstellen, oder Datenträger mit Datensicherungen entsprechend an einem ausgelagerten Ort aufzubewahren.

Die folgenden Beispiele können Maßnahmen der Verfügbarkeitskontrolle darstellen:

- Anschaffung eines Notstromaggregats
- Klimananlage
- Feuersicherer Serverraum
- Installation von Brand- und Rauchmeldern
- Schutzsteckdosenleisten mit Überspannungsschutz
- Alarmanlagen zur Diebstahlsicherung
- Externe Aufbewahrung von Sicherheitskopien
- Erstellung eines Datensicherheitskonzepts
- Regelmäßige Tests der erstellten Backups (Test der Restore-Funktion)

Nr. 8 - Datentrennung

Zu unterschiedlichen Zwecken erhobene personenbezogene Daten müssen natürlich auch getrennt ausgewertet werden können. Diesem Erfordernis wird das Datentrennungsgebot gerecht, welches organisatorische technische Maßnahmen zur Datentrennung verlangt. Getrennt werden müssen Beispielsweise Mitarbeiter- und Kundendaten, oder auch die Daten verschiedener Kunden bei einem Auftragsdatenverarbeiter. Eine physikalische Trennung (verschiedene Datenträger) ist jedoch nicht immer umsetzbar oder wirtschaftlich sinnvoll. Es ist daher ausreichend wenn die Daten logisch getrennt voneinander gespeichert werden. Dafür ist es ausreichend wenn die Daten beispielsweise nur über verschiedene Zugangsdaten erreichbar sind.

Andere Möglichkeiten der Datentrennung wären:

- Einsatz verschiedener Datenbanken
- Einsatz von Zugriffskontrollsoftware und Einrichtung von Zugriffsrechten
- Verschiedene Verschlüsselung für einzelne Datensätze