Anlage 3

Technisch-organisatorische Maßnahmen
Mittelrhein LastMile Express GmbH, Koblenz

---

1. Vorbemerkung

Die Generalklausel des Art. 24 und 32 DS-GVO verpflichtet die Mittelrhein LastMile Express GmbH als Verantwortlicher im Sinne datenschutzrechtlicher Bestimmungen, geeignete technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen, dass die Verarbeitung der personenbezogenen Daten datenschutzkonform erfolgt. Konkretisiert wird dies insbesondere in den Art. 25, 32 und 35 DS-GVO.

Dieses technisch-organisatorische Konzept dient dem Zweck, die rechtliche Umsetzung der allgemeinen und besonderen technischen und organisatorischen Maßnahmen sicherzustellen.

Sowohl zum Zeitpunkt der Festlegung der Mittel als auch zum Zeitpunkt der eigentlichen Verarbeitung (insbesondere IT Systeme und Software) müssen geeignete technische und organisatorische Maßnahmen getroffen werden, um den Datenschutzgrundsätzen, den Garantien der DS-GVO sowie den Betroffenenrechten zu genügen.

Demnach soll die Technik als Mittel zur Durchsetzung des Datenschutzrechts eingesetzt werden.

In diesem Zusammenhang sind insbesondere der Stand der Technik sowie die Implementierungskosten zu beachten. Im Hinblick auf den Stand der Technik dürften grundsätzlich die „besten verfügbaren Techniken“ gemeint sein, die auf gesicherten wissenschaftlichen und technischen Erkenntnissen beruhen und darüber hinaus realistisch verfügbar sind. Natürlich sind diesbezüglich auch die Implementierungskosten zu berücksichtigen. Es besteht die Möglichkeit, nicht auf die wirksamste verfügbare technische Maßnahme zurückzugreifen, wenn diese unangemessene Kosten verursachen würde, mithin unverhältnismäßig wäre.

Ferner sind als begrenzende Faktoren zu berücksichtigen:

- Art, Umfang, Umstände und der Zweck der Verarbeitung,
- unterschiedliche Eintrittswahrscheinlichkeit und die
- Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen.

Durch geeignete technische und organisatorische Maßnahmen muss in den bei der Mittelrhein LastMile Express GmbH eingesetzten IT Systemen und der Software sichergestellt werden, dass durch Voreinstellungen nur die erforderlichen personenbezogenen Daten verarbeitet werden. Dies gilt insbesondere im Hinblick auf

- die Menge der Daten,
- den Umfang der Verarbeitung,
- die Speicherfrist und
- die Zugänglichkeit nebst der Verhinderung der Zugänglichkeit.

Während aus Art. 25 Abs. 1 DS-GVO („*Privacy by design*“) für den Verantwortlichen die Pflicht folgt, entsprechende Einstellungs- und Kontrollmöglichkeiten systemseitig vorzusehen, verlangt der Grundsatz des „*Privacy by default*“ gemäß Art. 25 Abs. 2 DS-GVO, bei vorhandenen Einstellungsmöglichkeiten „ab Werk“ den Grundsatz der Datenminimierung zu berücksichtigen.

Dieser Grundsatz verlangt demnach, dass Nutzer keine Änderungen an den Einstellungen vornehmen müssen, um eine möglichst datensparsame Verarbeitung zu erreichen. Vielmehr soll umgekehrt jede Abweichung von den datenminimierenden Voreinstellungen erst durch ein aktives Eingreifen der Nutzer möglich werden.

Art. 25 Abs. 2 DS-GVO ist durch den Maßstab der Erforderlichkeit der Datenverarbeitung begrenzt. Demnach ist nicht zwingend die datenschutzfreundlichste Voreinstellung zu wählen. Vielmehr kann auch eine datenintensive Voreinstellung zulässig sein, solange der Verarbeitungszweck dies erfordert.

Unter Maßgabe dessen ist bei der Mittelrhein LastMile Express GmbH das nachfolgende technisch-organisatorische Konzept entwickelt worden.

2. Technisch-organisatorisches Konzept

Der Datenschutz insb. der Kundendaten (Abonnenten) und der sonstigen bei der Mittelrhein LastMile Express GmbH verarbeiteten personenbezogenen Daten wird im Rahmen der Datensicherheit und Integrität der Verarbeitung wie folgt abgesichert, wobei dieses Konzept aufgrund technischer Weiterentwicklungen und künftiger Gefährdungen stetig überprüft und weiterentwickelt wird.

Die Mittelrhein LastMile Express GmbH verfügt über einen betrieblichen Datenschutzbeauftragten und IT-Systemadministratoren, die schriftlich auf das Datengeheimnis verpflichtet sind.

Basis des Konzepts ist eine Dokumentation der technischen und organisatorischen Maßnahmen bei der Mittelrhein LastMile Express GmbH, die am 25.05.2018 stattgefunden hat.

2.1. Zutrittskontrolle:

Im Rahmen der Zutrittskontrolle werden nachfolgend die Maßnahmen dargestellt, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verwehrt werden soll:

- Die zentralen Serveranlagen stehen in zwei Räumen im Verwaltungsgebäude am Sitz der Mittelrhein-Verlag GmbH (Konzernmuttergesellschaft) in der Mittelrheinstr. 2-4, 56072 Koblenz sowie in zwei Räumen im Druckhaus, Mittelrheinstr. 2, 56072 Koblenz (jeweils ein Backup). Diese sind durch Brandmeldeanlagen und teilweise durch Rauchabsaugsysteme und Gaslöschanlagen geschützt. Des Weiteren wird eine elektronische Schließanlage (Codeschloss) gegen den Zutritt Unbefugter eingesetzt.

- Die Schlüsselgewalt (einschließlich der Vergabe von Zutrittsrechten) wird durch folgende Personen ausgeübt: IT Systemadministratoren

- Regelmäßigen Zugang haben folgende Personen: Geschäftsleitung, Haustechnik, Infrastrukturteam und IT-Mitarbeiter. Dies gilt für Rechenzentrum und Serverräume.

- Weitere Personen, die Zutritt verlangen, werden im Rahmen einer Zutrittskontrolle einer Legitimationsprüfung unterzogen und sodann in einem fortlaufenden Verzeichnis dokumentiert. Gleiches gilt für die Anwesenheit über das Codeschloss. Dies geschieht primär durch den Pförtner und sodann über eine Schlüsselregelung.

- Sämtliche laufend zutrittsberechtigten Personen sind auf das Datengeheimnis schriftlich verpflichtet.

- Nachts ist das Gebäude durch einen Wachschutz einbruchgesichert.

2.2. Zugangskontrolle:

Im Rahmen der Zugangskontrolle geht es um die Darstellung von Maßnahmen, die eine Nutzung von Datenverarbeitungsanlagen durch Unbefugte verhindern sollen.

- Die Mittelrhein-Verlag GmbH trifft als Konzernmuttergesellschaft und als zuständiger IT-Dienstleister der Mittelrhein LastMile Express GmbH zunächst Maßnahmen zur Benutzeridentifikation und Authentifizierung von Nutzern im Zuge der Anmeldung zu Datenverarbeitungsanlagen. Diese Nutzer müssen sich unter einem bei der Mittelrhein-Verlag GmbH registrierten Klarnamen und einem individuellen Passwort melden. Die Anmeldung wird über die EDV protokolliert. Über die Nutzung der Passwörter werden die Mitarbeiter geschult. Es existiert eine Passwortrichtlinie (PN-Police). Die Passwörter werden im 365 Tage Turnus gewechselt. Sie haben eine Mindestlänge von 8 Zeichen und werden nur verschlüsselt abgespeichert oder übertragen (Active Directory). Es existiert eine Passworthistorie. Nach 15 erfolglosen Anmeldungen wird der Zugriff automatisch gesperrt. Bei Arbeitsunterbrechungen wird ein passwortgeschützter Bildschirmschoner aktiviert.

- Die Administratorpasswörter werden gesichert aufbewahrt. Gleiches gilt für Schlüssel für Kryptographieverfahren.

- Die Netzwerkorganisation ist so aufgebaut, dass der Zutritt immer nur zu einem für den Zugriff zugelassenen Segment erfolgt. Die Datenbankstruktur ist mandantenbasiert dergestalt aufgebaut, dass der Zugriff nach der Authentifizierung nur in einem hierfür zugelassenen Segment erfolgen kann, das auf den Nutzer („Mandanten“) zugelassen ist.

- Die IT-Systeme werden über eine verschlüsselte Standleitung (MPLS/VPN Standard) gegen unbefugte Nutzung geschützt.

- Mobile Endgeräte (Smartphones/Tablets etc), die personenbezogene Daten enthalten oder den Zugriff hierauf ermöglichen, sind gerätebezogen über ein Passwortsystem verschlüsselt.

- Arbeitnehmer, die solche mobilen Endgeräte des Verantwortlichen einsetzen, unterliegen einer arbeitgeberseitigen Weisung zur Nutzung dieser Endgeräte, die insb. auch die zur Nutzung zugelassene Software (einschließlich Apps) beschreibt. Hierzu wird auch ein Mobile Device Management-System eingesetzt.

- Es kann nur freigegebene Software genutzt werden.

2.3. Zugriffskontrolle:

Die zum Zugriff auf Daten der Datenverarbeitungsanlagen der Mittelrhein LastMile Express GmbH Berechtigten sollen nach dem sog. *need-to-know*-Prinzip nur auf die personenbezogenen Daten zugreifen können, zu denen eine Berechtigung besteht.

- Die Mittelrhein-Verlag GmbH hat ein Konzept der Berechtigungen der einzelnen Personen mit Zutrittsrechte zu Datenverarbeitungsanlagen erstellt. Dies ist in sog. Gruppenrichtlinien dokumentiert, die hierarchisch (Geschäftsleitung/Disziplinarvorgesetzter/Fachvorgesetzter) umgesetzt werden. Die Vergabe der Zugriffsrechte erfolgt durch die IT Administratoren.

- Nach Anmeldung mit Name und Passwort besteht ein Zugriffsrecht nur zu den individuell zugeschlüsselten Programmrechten des Systems. Diese Rechte werden rollenbasiert ausgehend von der Funktion der betreffenden Person automatisch über die IT Anlagen gesteuert.

- Im Rahmen dieser Steuerung werden auch die einzelnen Rechte der betroffenen Personen definiert: „lesen/ändern/löschen/drucken/exportieren/mailen“.

- Eine Änderung dieser Profile wird im Einzelfall durch den IT-Verantwortlichen (ggfls. nach Einbindung des Datenschutzbeauftragten) vorgenommen.

2.4 Weitergabekontrolle:

Im Rahmen der Weitergabekontrolle werden die Maßnahmen dargestellt, die im Rahmen einer elektronischen Übertragung während des Transports oder bei der Speicherung verhindern sollen, dass Unbefugte solche personenbezogenen Daten lesen, kopieren, verändern oder entfernen können. Des Weiteren soll festgestellt werden, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Es wird zunächst eine Mindestverschlüsselung unter Einhaltung folgender Standards im Rahmen eines Netzwerkprotokolls gesichert:
    - Es gibt eine Firewall, ein Intrusion Detection System, ein Intrusion Prevention System und ein VPN (Virtual Private Network) als Schutzmaßnahmen technischer Art.
    - Die Daten werden über eine gesicherte Standleitung transportiert.
    - Die Mails und unsere Internetseiten sind SSL/TLS verschlüsselt.

- Bei Risikodaten erfolgt nach Maßgabe des Benutzers eine weitere Verschlüsselung für den Transport der Daten (z.B. Bildung einer mit Passwort gesicherten ZIP-Datei), wobei das Passwort nach Identifikation des Nutzers separat mitgeteilt wird.

- Seriendateien an mehrere Empfänger werden mit einer Verschlüsselung der Empfängeradressen versendet.

- Ungenutzte Datenträger werden in einem Safe aufbewahrt. Ausgeschiedene Mitarbeiter werden hinsichtlich der Nutzungsrechte gesperrt.

- Die Datenvernichtung erfolgt durch einen zertifizierten Entsorger.

- Externe Dienstleister sind auf das Datengeheimnis verpflichtet. Diese werden bei ihren Arbeiten beaufsichtigt. Dies gilt auch bei Fernwartungen, die im Einzelfall vom Administrator freigegeben werden. Vor Wartungen erfolgt eine Sicherung der Daten.

2.5. Eingabekontrolle:

Im Rahmen der Eingabekontrolle sollen Maßnahmen ergriffen werden, die eine nachträgliche Überprüfung und Feststellung der Personen, die auf personenbezogene Daten zugegriffen haben, ermöglicht.

- Die Mittelrhein-Verlag GmbH trifft technische Maßnahmen, die eine nachträgliche Überprüfung, ob und wer auf personenbezogene Daten zugegriffen hat, ermöglicht.

- Dies geschieht über technische Vorkehrungen zu einer Änderungshistorie einschließlich einer Dokumentation der Zugriffszeit und der Person, die zugegriffen hat.

- Die so gewonnenen Daten über die Zugriffe, die ihrerseits wieder personenbezogene Daten sind, werden nur für diesen Zweck abgespeichert und genutzt. Eine Nutzung zu anderen Zwecken, insbesondere zu Zwecken einer allgemeinen anlasslosen Überwachung der zugreifenden Personen ist ausgeschlossen.

- Ein Zugriff auf diese Änderungs- und Zugriffhistorie setzt einen Anlass voraus und findet unter Einbindung des IT-Verantwortlichen, des Datenschutzbeauftragten und ggf. des Betriebsrates statt. Es erfolgt eine Dokumentation.

- Es gibt einen Schadsoftwareschutz, der automatisch durch Updates aktualisiert wird. Dies geschieht spätestens 1 Tag nach Herstellerinformation.

- Die Verfügbarkeit wird täglich über Backups sichergestellt. Dies geschieht auf Basis eines Backup-Plans durch Festplattenspiegelung, SAN Snapshots, Havariearchivierung, unterbrechungsfreie Stromversorgung und Überspannungsfilter. Verantwortlich ist ein Backup-Administrator. Dies wird durch Rufbereitschaft gesichert.

- Die Backup-Sicherungen werden in einem Tresor aufbewahrt, der in einem anderen Brandabschnitt steht.

2.6. Auftragskontrolle:

Im Rahmen der Auftragskontrolle wird geprüft, ob alle Personen, insb. Auftragsverarbeiter im Sinne von Art. 28 DS-GVO, die personenbezogenen Daten gesetzeskonform verarbeiten, insbesondere Maßnahmen ergriffen sind, die die Einhaltung von Weisungen der Mittelrhein LastMile Express GmbH sichern.

- Sämtliche Arbeitnehmer und freien Mitarbeiter sind schriftlich auf das Datengeheimnis verpflichtet.

- Auftragsverarbeiter im Sinne von Art. 28 DS-GVO sind angehalten, die dort ergriffenen Maßnahmen zum Schutz personenbezogener Daten der Mittelrhein LastMile Express GmbH offenzulegen. Es ist ein Vertrag mit diesen Auftragsverarbeitern abgeschlossen, der den gesetzlichen Vorgaben entspricht und insb. die Durchsetzung von Weisungen sichert. Auftragsverarbeiter werden entsprechend der möglichen Risiken überprüft.

3. Datenschutzrechtliche Einstellungen:

- Voreinstellungen in den Datenverarbeitungsanlagen der Mittelrhein LastMile Express GmbH dienen dazu, die datenschutzrechtlichen Vorgaben umzusetzen. Dies geschieht insb. zur Umsetzung des Grundsatzes der Datenminimierung, indem Löschprozesse im System eingepflegt sind, so dass Routinelöschszenarien greifen.

- Weiterhin ist in den Datenverarbeitungssystemen über Zugriffsroutinen sichergestellt, dass gesetzliche Informationspflichten insb. aus Art. 13 und 14 DS-GVO (etwa durch sog. Fernzugriff) gegenüber den Informationsadressaten erfüllt werden können.

4. Weiterentwicklung:

Dieses Konzept technisch organisatorischer Maßnahmen wird laufend vom IT Verantwortlichen insb. hinsichtlich des Standes der eingesetzten technischen Mittel überprüft und in Abstimmung mit der Leitung des Verantwortlichen unter Berücksichtigung der gesetzlichen Anforderungen von Art. 24 und 25 DS-GVO fortentwickelt.

5. Inkrafttreten:

Dieses technisch-organisatorische Konzept tritt am 25.05.2018 in Kraft.

Stand 05/2018