FLYMINT®

INFORMATIONEN ZUM DATENSCHUTZ

Stand Februar 2014

Flymint GmbH

Leutragraben 1
07743 Jena, Germany
Tel. +49 3641 573 34 00
Fax +49 3641 573 34 03

Die nachfolgenden Informationen beschreiben technische und organisatorische Maßnahmen zum Datenschutz sowie den Umgang mit personenbezogenen Daten durch die Flymint GmbH.

Die erläuterten Maßnahmen und Bestimmungen gründen sich auf die gesetzlichen Regelungen entsprechend §9 BDSG und Anlage sowie §11 BDSG.

1. Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Die Flymint GmbH gewährleistet die folgenden technischen bzw. organisatorischen Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- ✓ Das Gebäudekonzept des Intershop Towers ermöglicht die Absicherung der Räumlichkeiten vor Publikumsverkehr durch die Vermietergesellschaft
- ✓ Der Intershop Tower verfügt über das nötige Zutrittskontrollsystem in Form einer Personenseparierungsanlage an den Fahrstühlen und von Chipkarten für den Etagenzutritt
- ✓ Überwachungseinrichtungen in Form von Videokameras am Empfang und Außenbereich sichern zusätzlich den Zutritt ab.
- ✓ Die Schlüssel zur Schließanlage wurden durch den Geschäftsführer vergeben und sind ausschließlich den hiermit betrauten Mitarbeiter zugänglich. Die Ausgabe der Schlüssel wird im Schlüsselbuch protokolliert.
- ✓ Die Lobby des Intershop Towers sichert den Zutritt durch weiteres Personal ab. Pförtner sind für den Wachschutz zuständig.
- ✓ Fremdpersonal, wie bspw. Reinigungspersonal, wird der Zutritt zu den Büroräumen nur unter Anwesenheit von Mitarbeitern gewährt.
- ✓ Sicherheitsbereiche, wie bspw. der Serverraum, der zusätzlich einen Panzerschrank beherbergt, sind durch separierte Schlüssel und Zutrittsprotokollierung geschützt.
- ✓ Die Backup-Aufbewahrung der PURLs wird durch den Server-Hoster Domainfactory gewährleistet.
- ✓ Die Backup-Aufbewahrung im Büro wird durch redundante Sicherungen im Truecryptcontainer des NAS gewährleistet.

- ✓ Die Datenträgeraufbewahrung durch Festplatten erfolgt auf Arbeitsplatzrechnern, welche in abschließbaren Räumen
- ✓ Die gefertigten Briefe (Lettershop Geschäftsfeld) werden in abschließbaren Schranksystemen gelagert.

2. Zugangskontrolle

Das Eindringen Unbefugter in die Datenverarbeitungssysteme ist zu verhindern.

Technische (Kennwort-/ Passwortschutz) und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung sind:

- ✓ Die unbefugte Nutzung der Bürodatenverarbeitung wird durch Nutzererkennung und Passwortschutz mit hoher Passwortgüte sowie der Zuordnung der Nutzer zu einem Account verhindert. Die Bildschirmsperre tritt nach 15min mit Login-Aufforderung ein. Die Funktionstrennung der Zugriffssteuerungsliste (ACL) wird für Kommuniaktionsprotokollfreigaben (SMB-Freigabe) vorgenommen.
- ✓ Berechtigte Mitarbeiter verfügen über eigene, nur ihnen bekannte Passwörter.
- ✓ Die Passwortpolicy wird in Dienstvereinbarungen verbindlich festgelegt.
- ✓ Die Aktivitäten bezüglich der PURLs protokolliert (Server), so das Zurechenbarkeit und Revisionssicherheit gegeben sind.
- ✓ Alle Aktivitäten zur Datenübermittlung werden ebenfalls protokolliert, so das Zurechenbarkeit und Revisionssicherheit gegeben sind.
- ✓ Die Datenhaltung erfolgt in verschlüsselten Ordnern mit Authentifizierung.

3. Zugriffskontrolle

Unerlaubte Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

Eine bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung erfolgen durch:

- ✓ System- und Anwendungsautorisierungen werden vorgenommen mit entsprechenden Berechtigungskonzepten für Office und Onlinedienste.
- ✓ Die Berechtigungen für Datentransaktionen (Lesen/Löschen/Ändern) werden differenziert und auf die zur Aufgabenerfüllung notwendigen Rechte beschränkt.

- ✓ Die Berechtigungen für Daten, Anwendungen und Betriebssysteme werden ebenfalls differenziert.
- ✓ Die Berechtigungserteilung erfolgt getrennt, einerseits durch die Bewilligung des Geschäftsführers, andererseits durch die Vergabe durch den System Operator.
- ✓ Es gibt eine Regelung zur Wiederherstellung von Backups. Die Backupeinspielung ist erprobt und im Notfallplan festgelegt.
- ✓ Administrative Aktivitäten auf dem Server (Datei- und Anwendungsnutzung) werden weitgehend auf dem Produktivserver protokolliert.
- ✓ Die Nutzeraktivitäten im FLYMINT-Dialogtool werden innerhalb des Dialogtool-Backends protokolliert.
- ✓ Die Funktionstrennung von Test- und Produktionsumgebung wird durch getrennte Test- und Produktivserver ermöglicht.

4. Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten sind zu regeln. Hierzu zählen die elektronische Übertragung, der Datentransport sowie die Form der Übermittlungskontrolle.

Maßnahmen, die zur Sicherung des Transports, der Übertragung und Übermittlung oder Speicherung auf Datenträgern (manuell oder elektronisch) sowie der nachträglichen Überprüfung beitragen, sind:

- ✓ Bei der Übermittlung von Datensätzen erfolgt der Zugriff über separat geschützte Emailadressen.
- ✓ Die Übermittlung der Daten wird durch ein separates Datenverarbeitungsprotokoll geregelt. (siehe separate PDF zur Auftragsdatenverarbeitung)
- ✓ Befugte Mitarbeiter protokollieren den Ein- und Ausgang der Daten.
- ✓ Die administrative Verbindung zu Servern erfolgt ausschließlich über Secure Shell.
- ✓ Die Nutzerverbindung zum Dialogsystem erfolgt verschlüsselt via SSL-Zertifikat.
- ✓ Zugriff erfolgt nur durch berechtigte Mitarbeiter. Die wird durch eine Legitimationsprüfung sichergestellt.

5. Eingabekontrolle

Die Nachvollziehbarkeit/Prüfbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- ✓ Die Benutzerberechtigungen der Mitarbeiter sind differenziert und erfolgen nach dem Need-to-know-Prinzip (Kenntnis nur bei Bedarf).
- ✓ Die Benutzerberechtigungen der Nutzer sind differenzierbar.

6. Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

Maßnahmen (technisch/organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer sind:

- ✓ Ein geprüfter, dem Bundesdatenschutzgesetz entsprechender Vertrag zur Auftragsdatenverarbeitung wird vereinbart. (siehe separate PDF zur Auftragsdatenverarbeitung)
- ✓ Die Mitarbeiter werden durch den Arbeitsvertrag zur Geheimhaltung verpflichtet.
- ✓ Die Mitarbeiter werden zu den Erfordernissen des Datenschutzes durch Weiterbildungen, Merkblätter und Dienstvereinbarungen unterrichtet.
- ✓ Subunternehmer sind Domainfactory, IKS (zuständig für die Netzwerkadministration der Geschäftsräume) und Dokumentenvernichter.

7. Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zur Datensicherung (physikalisch/logisch) sind:

- ✓ Das Backup- und Wiederherstellungskonzept ermöglicht Backups durch eine BDSG-konforme Cloudlösung.
- ✓ Vereinbarungen bezüglich der Datenübergage werden separat in Auftragsdatenverarbeitungsverträgen geregelt.
- ✓ Redundanz sowie eine katastrophensichere Datenhaltung werden durch Domainfactory zugesichert.
- ✓ Die katastrophensichere Datenhaltung bezüglich der Brieffertigung und Aufbewahrung (Lettershop Geschäftsfeld) wird durch das Gebäudekonzept und durch verschlossene Schranksysteme gewährleistet.

8. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken sind:

- ✓ Es erfolgt eine Trennung der Auftraggeberdaten von anderen Klienten durch eine separate Verschlüsselung in der PURL.
- ✓ Unterschiedliche Klienten erhalten auch unterschiedliche Zugriffsteuerungslisten (ACL). Diese werden von den Klienten selbstständig festgelegt.
- ✓ Redundanz sowie eine katastrophensichere Datenhaltung werden durch Domainfactory zugesichert.