MY-LITFAX | PRINTROOM
Datenschutzkonzept
gemäß Art. 5 DSGVO

Das vorliegende Datenschutzkonzept hat zum Ziel, in einer zusammenfassenden Art die datenschutzrechtlichen Aspekte in Bezug auf das Unternehmen in Form einer Dokumentation darzustellen. Dabei dient es als Grundlage und der Unterstützung datenschutzrechtlicher Prüfungen im Rahmen der AV und gewährleistet und dokumentiert die Einhaltung datenschutzrechtlicher Bestimmungen wie der DSGVO.

Dieses Datenschutzkonzept wurde zuletzt geändert am 01.04.2022 um 13:30:00.

litfax® GmbH - Verlag für Banken
Sitz der Gesellschaft: Berlin
Darßer Bogen 3 - 13088 Berlin

Telefon: +49 (0) 30 / 688 1919-70
Telefax: +49 (0) 30 / 688 1919-99
E-Mail: info@my-litfax.de

Vertreten durch:
Peter Junge

Registereintrag:
Eingetragen im Handelsregister.
Registergericht: Berlin
Registernummer: HRB 96160B

Umsatzsteuer-ID:
Umsatzsteuer-Identifikationsnummer nach §27a Umsatzsteuergesetz: DE241211663

Das vorliegende wurde durch die Geschäftsführung (Peter Junge) genehmigt.

Datenschutzbeauftragter: DataCo GmbH

I. Einleitung und Ziele des Datenschutzkonzeptes

Die Softwarelösungen der Litfax GmbH sind nicht nur durch ihre Verbreitung im professionellen Umfeld, sondern insbesondere auch durch den Umfang und die Sensibilität der erfassten Daten in hohem Maße datenschutzrelevant.

Der damit verbundenen Verantwortung ist die Litfax GmbH sich selbstverständlich bewusst und hat zahlreiche Maßnahmen unternommen, um nicht nur den datenschutzrechtlichen Bestimmungen (z.B. der DSGVO) gerecht zu werden, sondern ein möglichst hohes und angemessenes Schutzniveau zu bieten.

1.1. Zum Unternehmen: Die Litfax GmbH – Verlag für Banken

Die Litfax GmbH – Verlag für Banken – nachfolgend „Litfax GmbH“ – wurde am 28.02.2005 in Berlin gegründet und verkauft seitdem Druckerzeugnisse und deren Personalisierung mit personenbezogenen Daten, über eine Softwarelösung im Bereich Web-to-Print OnlineShop-Lösung.

Um dieser verantwortungsvollen Aufgabe gewissenhaft nachzukommen, beschäftigt das Unternehmen derzeit ca. 10 Mitarbeiter am Standort Berlin. Die Geschäftsführung haben aktuell Peter Junge und Stefanie Junge inne.

Branche	Einzelhandel und Druckdienstleister
Gegenstand des Unternehmens	Umsetzung von Softwarelösungen im Bereich Web-to-Print, Handel / Herstellung von Druckerzeugnissen und Personalisierung

II. Dokumentation und Beschreibung des Verfahrens

Das Produkt „my-litfax | printroom“ ist eine individuelle Shop-Plattform, welche dazu geeignet ist, Web-to-Print-Dokumente zu erstellen (speziell Zahlungsverkehrsvordrucke und Visitenkarten). Hierbei werden im Rahmen des Bestellprozesses und der Personalisierung personenbezogene Daten erhoben und verarbeitet.

In der Standardanwendung ist hier die Verarbeitung personenbezogener Daten möglich, allerdings werden keine sensiblen Daten nach Art. 9 DSGVO Abs. 1 (z.B. rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder eine Gewerkschaftszugehörigkeit) erfasst oder verarbeitet.

In den Benutzerstammdaten können vom Benutzer selbst oder der Administration Bankdaten hinterlegt werden (Kontoverbindung).

Die Verwendung zur Verfügung gestellter Freifelder ist dem Benutzer überlassen, worüber grundsätzlich auch sensible Daten erfasst und in den hinterlegten Prozessen bzw. der Druckdatei verarbeitet werden kann.

Da im beschriebenen Standardverfahren der Software lediglich „nicht sensible“ personenbezogenen Daten verarbeitet werden, beschränkt sich die Anforderung an die notwendigen technischen und organisatorischen Maßnahmen (kurz „TOMs“), die gemäß Art. 32 DSGVO getroffen werden müssen.

2.1. Datenschutzpolitik und Verantwortlichkeiten im Unternehmen

Verantwortliche Stelle	Litfax GmbH – Verlag für Banken Darßer Bogen 3 13088 Berlin Telefon: 030 / 688 1919 – 70 Telefax: 030 / 688 1919 – 99
Geschäftsführung	Herr Peter Junge Frau Stefanie Junge
Technische Leitung	Herr Ayhan Sert (extern)
Datenschutzbeauftragter	DataCo GmbH - externer Datenschutzbeauftragter – Telefon: 089 / 7400 45840 E-Mail: datenschutz@litfax-bv.de
Datenschutzkoordination	Herr Peter Junge - interner Datenschutzkoordinator – Telefon: 030 / 688 1919 -70 E-Mail: datenschutz@litfax-bv.de

2.2. Produktbeschreibung und Zweck der Software (OnlineShop – my-litfax.de) und der Verarbeitung

Der my-litfax OnlineShop ist eine multilinguale, webbasierte Web-to-Print-Lösung, die speziell für den B2B-Bereich zur Firmenkundenbetreuung konzipiert wurde, aber auch für den B2C Bereich genutzt werden kann.

Alle Abläufe – von der Auftragsannahme über die Erstellung inklusive aller Korrekturschleifen bis hin zur Genehmigung und Freigabe werden vollständig online abgebildet und innerhalb weniger Minuten abgewickelt – jederzeit und von nahezu jedem Ort der Welt.

Selbst die Druckauftragsbearbeitung und –produktion kann vollautomatisiert werden. Die my-litfax Lösungen sind entweder als kostenfreie oder Lizenz-Version verfügbar.

Personenbezogene Daten werden zum Zweck der Bestellabwicklung und Personalisierung von Produkten erfasst und genutzt. Hierzu zählt unter anderem auch die ggf. anschließende Weiterleitung der Daten an weitere, durch ggf. verknüpfte Dienstleister, sofern dies erforderlich ist.

2.3. Art der personenbezogenen Daten

Die Art der verarbeiteten personenbezogenen Daten ergibt sich aus dem Hauptvertrag und umfasst folgende Datenarten / -kategorien:

- ✓ Personen- bzw. Unternehmensstammdaten
- ✓ Kontodaten (IBAN, Kontoinhaber, Schecknummer)
- ✓ Kommunikationsdaten
- ✓ Vertragsstamm- und Bestelldaten
- ✓ Kundenhistorie
- ✓ Vertragsabrechnungs- und Zahlungsdaten
- ✓ Planungs- und Steuerungsdaten
- ✓ Verbindungsdaten (IP-Adresse)
- ✓ Benutzer- und Zugangsdaten
- ✓ Bildmaterial (Inhalt durch Auftraggeberin bestimmt)

Diese Auflistung umfasst Standardprozesse der Software. Die Auftraggeberin hat innerhalb der Software die Möglichkeit, individuelle Felder anzulegen und somit weitergehende Daten zu erfassen.

2.4. Kategorien betroffener Personen

die Auftragsverarbeitung umfasst die folgenden Kategorien betroffener Personen:

- ✓ Kunden (Privatkunden und Firmenkunden)
- ✓ Interessenten, Handelsvertreter
- ✓ Beschäftigte, Ansprechpartner
- ✓ Lieferanten, Handelsvertreter
- ✓ Externe Dienstleister

2.5. Empfänger von Daten

In der Regel sehen nur die Nutzer die zur Verfügung gestellten Daten (also Endkunden und Mitarbeiter der Litfax GmbH). Seitens der Litfax GmbH ist ein Zugriff von externen Programmierer und / oder Rechenzentrumsbetreiber nicht auszuschließen. Dies findet im Rahmen von Auftragsdatenverarbeitungen gemäß Art. 28 DSGVO statt.

2.6. Regelfristen für die Löschung der Daten

Innerhalb der Software von my-litfax gelten folgende Löschfristen:

Zugangs- und Benutzerstammdaten	Manuelle Löschung bzw. Sperrung des für 4 Wochen z.B. einer Kündigung
Temporäre serverseitig von der Software generierte Daten	2 Tage / 24 Stunden
Temporär generierte Druckdaten	30 Tage
Logfiles (SQL & Upload)	2 Tage

Über das Backend gelöschte Datensätze werden i. d. R. unmittelbar aus der Datenbank gelöscht oder einem Löschscript hinzugefügt. Ggf. erstellte Backups bleiben von diesen Löschfristen unberührt.

2.7. Übermittlung an Drittstatten

Litfax GmbH nimmt seine datenschutzrechtliche Verantwortung sehr ernst und übermittelt keine Daten an Stellen in Drittstaaten. Eine derartige Übermittlung ist auch nicht geplant. Der Datenverkehr wird außerdem im Backend verschlüsselt übertragen und ist auch im Frontend mit einem SSL-Zertifikat versehen.

2.8. Einschätzung bzgl. Des Schutzbedarfs der Daten

Im nachfolgenden Kapitel werden die getroffenen Schutzmaßnahmen im Rahmen der technischen und organisatorischen Maßnahmen genauer beschrieben.

Für die Daten, die Rahmen der Nutzung der Software my-litfax erfasst werden gilt:

1. Die Daten fallen **nicht** unter die Kategorisierung sensibler Daten nach Art. 9 Abs. 1 DSGVO.
2. Die Daten unterliegen **nicht** dem Sozialdatenschutz gemäß. § 67 ff. SGB X.
3. Die Daten unterliegen **nicht** der beruflichen Schweigepflicht gemäß § 203 StGB („Verletzung von Privatgeheimnissen“).
4. Die Daten umfassen Details zur geschäftlichen Tätigkeit des Auftraggebers und unterliegen somit dem GeschGehG (Geschäftsgeheimnisgesetz).

Die Einschätzung kann darüber hinaus auch anhand von bewährten Klassifizierungen eingeschätzt werden. Im Fall dieser Software sind folgende Zuordnungen zutreffend:

1. Gemäß der schutzstufen der Landesdatenschutzbeauftragten fallen die Daten in die **Stufe C** („Personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann (Ansehen), z.B. Einkommen, Sozialllleistungen, Grundsteuer, Ordnungswidrigkeiten“).

2. Gemäß den Anforderungen zur Vernichtung von Datenträgern (DIN 66399-1) handelt es sich um die **Sicherheitsstufe 3** („Anwendbar bei Datenträgern mit sensiblen und vertraulichen Daten sowie personenbezogenen Daten, z.B. Umsatzauswertungen und Steuerunterlagen von Unternehmen sowie Angebote, Bestellungen etc. mit Adressdaten von Personen.“).

3. Gemäß einer anderen Klassifizierung gehören die Daten der **„Sozialsphäre“** an („Das, was auch von Menschen wahrgenommen werden kann, zu denen keine persönlichen Beziehungen bestehen. Es geht als z.B. um die beruflichen Tätigkeit, die Anwesenheit bei Veranstaltungen oder der Spaziergang durch eine Geschäftsstraße“).

Abschließend kann folgende Einschätzung bzgl. Des Schutzbedarfs der Daten abgegeben werden:

Nach Abwägung aller zur Verfügung stehenden Kriterien lässt sich feststellen, dass die vom my-litfax-Shop genutzten Daten allein aus dem geschäftlichen bzw. beruflichen Umfeld stammen. Betroffen ist ausschließlich die Sozialsphäre. Der datenschutzrechtlich erforderliche Schutzbedarf ist also als „niedrig“ einzuschätzen.

III. Allgemeine Maßnahmen zum Datenschutz

Die wirksame Einhaltung der datenschutzrechtlichen Bestimmungen und insbesondere der DSGVO erfordert eine reihe konkreter Maßnahmen wie die folgenden Punkte aufzeigen.

3.1. Bestellung eines Datenschutzbeauftragten

Litfax GmbH ist nach § 38 BDSG zur Bestellung eines Datenschutzbeauftragten verpflichtet und ist dieser Pflicht durch die Bestellung eines externen Datenschutzbeauftragten nachgekommen:

DataCo GmbH
- externer Datenschutzbeauftragter -
Dachauer Str. 65
80335 München
Deutschland
+49 (0) 89 / 7400 45840
datenschutz@dataguard.de

Der externe Datenschutzbeauftragte ist ein Datenschutzexperte, der nicht direkt im Unternehmen arbeitet, sondern als externer Dienstleister hinzugezogen wird. Ein externer Datenschutzbeauftragter weist aufgrund seiner Ausbildung und Erfahrung hohe Expertise im Datenschutzrecht auf und füllt die Rolle des Datenschutzbeauftragten (DSB) vollumfänglich aus.

- Geprüfter & zertifizierter DSGVO-Experte
- Branchenspezifische Datenschutzexpertise
- Persönliche und individuelle Beratung

3.2. Datenschutz-Schulung der Mitarbeiter nach Datenschutzrichtlinie

Zusätzlich zur allgemeinen Verpflichtung auf die Vertraulichkeit ist eine Sensibilisierung und Schulung der Mitarbeiter auf die jeweiligen Erfordernisse gefordert.

Die Mitarbeiter wurden vom Datenschutzbeauftragten persönlich geschult. Hierbei wurden folgende Themen geschult: Datenschutzpannen, Beispiele aus dem geschäftlichen Alltag, Datenschutzrecht, Historie des Datenschutzes, betroffene Personen und deren Daten, Bußgelder und Haftstrafen, Datenschutzmaßnahmen im Allgemeinen (Beschreibung der technisch-organisatorischen Maßnahmen gemäß Art. 32 DS-GVO) und im speziellen (Datenschutz am Computer und mit Akten).

3.4. EDV-Nutzungsvereinbarung

Es ist dem Datenschutz förderlich, wenn die Mitarbeiter ausführlich über den konkreten und datenschutzkonformen Umgang mit der Unternehmens-EDV (und ggf. vorhandenen Papierunterlagen) geschult werden. Hierzu wird aktuell eine entsprechende, unternehmensübergreifende EDV-Nutzungsvereinbarung erarbeitet und zusätzlich zu den regelmäßigen Schulungen allen Mitarbeitern ein entsprechendes Leitbild an die Hand gegeben.

3.5. Hard- und Software entsprechen dem „Stand der Technik“

Litfax GmbH setzt ausschließlich geprüfte, aktuelle Markengeräte (z.B. Apple, Dell, HP, Brother, Xerox, Reiner) ein. Für das Dokumentenmanagement werden Produkte der Schuchert Managementberatung GmbH eingesetzt wie z.B. Factro (Projektmanagement, interne Kommunikation – keine personenbezogenen Daten oder Zugänge, insbesondere zu Systemen mit Zugang zu personenbezogenen Daten). Alle Systeme werden regelmäßig und zeitnah auf dem aktuellen Stand gehalten.

3.6. Qualifikation der Mitarbeiter

Alle Mitarbeiter des Unternehmens wurden im Rahmen einer initialen Datenschutzschulung auf die Rechte und Pflichten im Datenschutz hingewiesen und auf die Vertraulichkeit verpflichtet. Aktuell wird zusätzlich eine entsprechende, unternehmensübergreifende EDV-Nutzungsvereinbarung erarbeitet.

Schulungsunterlagen sind für jeden Mitarbeiter in einem internen Bereich einsehbar und Rückfragen können direkt mit einem internen Datenschutzkoordinator oder den externen Datenschutzbeauftragten geklärt werden.

Die Schulung wird in regelmäßigen Abständen wiederholt, so dass neue Regelungen oder Optimierungen zeitnah in dem Unternehmen etabliert werden können.

3.7. Subunternehmen

Im EDV-Bereich ist eine Auslagerung spezieller, hochqualifizierter Aufgabenbereiche an externe Spezialisten empfehlenswert. Hierdurch wird die bestmögliche Fachkompetenz und Verfügbarkeit gesichert. Dies wird auch im Rahmen dieser Softwarelösung praktiziert.

Alle im Folgenden beschriebenen Auslagerungenfinden im Rahmen von Auftragsverarbeitungen gemäß Art. 28 DSGVO statt. Die Unter-Auftragnehmer sind entsprechend schriftlich verpflichtet.

(extern) Server-Betrieb durch die Host Europe GmbH oder Hostway Deutschland GmbH

Die Lizensierte Software (Multimandatensystem) wird ausschließlich auf Servern in Rechenzentren der Hostway Deutschland GmbH oder Host Europe GmbH gehostet. Durch die dort bestehende IT-Infrastruktur eines großen Rechenzentrum- und Server-dienstleisters wird eine optimale Betreuung der Hard- ggf. Software gewährleistet. Somit ist de Software im Regelfall rund um die Uhr sicher verfügbar.

(intern) Server-Betrieb durch die Litfax GmbH – Verlag für Banken

Server wird intern gehostet und gewartet. Durch die intensive Betreuung der Hard- und ggfs. Software wird eine optimale ausreichender Schutz gewährleistet. Somit ist die Hardware und Software im Regelfall rund um die Uhr sicher verfügbar.

Support-Unterstützung durch externe EDV-Fachkräfte (Herr Sert-externer Server- und Herr Koch –interner Server-)

IV. Technische und organisatorische Maßnahmen

Die vollständigen und aktuellen technischen und organisatorischen Maßnahmen können jederzeit bei der Litfax GmbH angefragt werden.

Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität

1.1.a Zutrittskontrollmaßnahmen zu Serverräumen (extern)

- ✓ Alle personenbezogenen Daten werden in einem Rechenzentrum eines unter Auftragnehmers gespeichert. Die DS-GVO-konforme Datenverarbeitung wurde zugesichert und Verträge zur Auftragsdatenvereinbarung wurden geschlossen.
- ✓ Hosting im Rechenzentrum der Hostway Deutschland GmbH, Standort Hannover

1.1.b Zutrittskontrollmaßnahmen zu Serverräumen (intern)

- ✓ Kein Zutritt fremder Personen zu den Geschäftsräumen und Serverraum
- ✓ Zugang nur nach vorheriger Terminabsprache, sowie Anmeldung und Sichtkontrolle über Gegensprechanlage
- ✓ Eintragung in Besucherliste
- ✓ Sicherung durch Codeschloss
- ✓ Sicherung durch Videoüberwachung

1.2 Zutrittskontrollmaßnahmen zu Büroräumen

- ✓ Die Büroräume befinden sich im Darßer Bogen 3, 13088 Berlin
- ✓ Die Nutzung von Schlüsselmaterial durch Mitarbeiter erfolgt gemäß Belehrung und dem zu unterschreibenden Schlüsselprotokoll
- ✓ Der Zugang für Besucher wird nur nach vorheriger Terminabsprache, sowie Anmeldung und Sichtkontrolle über die Gegensprechanlage am Haupteingang gewährt. Besucher tragen sich in einer Besucherliste ein
- ✓ Der Zugang für Postzusteller erfolgt nach vorheriger Anmeldung über das Rolltor der Produktionshalle. Die Produktionshalle selbst dürfen Postzusteller/Lieferanten in Begleitung durch Mitarbeiter der Versandabteilung der Litfax GmbH maximal 2 Meter betreten
- ✓ Die Räumlichkeiten werden außerhalb der Arbeitszeit videoüberwacht und alarmgesichert. Neben mehreren Kameras sind Bewegungsmelder, Brandmelder und Tür- sowie Fensterkontaktmelder vorhanden.
- ✓ Betriebsfremde Personen werden am Eingang vom jeweiligen Ansprechpartner abgeholt
- ✓ Zutrittsrechte werden personifiziert vergeben und können jederzeit widerrufen werden

1.3. Zugangs- und Zugriffskontrollmaßnahmen

- ✓ Es existiert ein definierter Freigabeprozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigung bei der Neueinstellung und beim Ausscheiden von Mitarbeitern
- ✓ Vergabe und Änderungen von Zugriffsrechten werden protokolliert
- ✓ jeder Mitarbeiter verfügt über eine individuelle Kennung zum Zugriff auf zentrale Verzeichnisdienste
- ✓ Es wurden verbindliche Passwort Richtlinien im Unternehmen festgelegt
- ✓ Bildschirme werden bei Inaktivität automatisch gesperrt oder ausgeschaltet
- ✓ Bei Verlust eines Zugangs werden Passwörter von der Administration neu vergeben
- ✓ Fernzugriff sind nur von berechtigten Mitarbeitern möglich und erfolgen über einen eindeutigen, sicheren SSH-Key
- ✓ Alle Serverzugriffe und -aktivitäten werden protokolliert
- ✓ Fernzugriffe werden bei Inaktivität automatisch getrennt
- ✓ alle Systeme werden durch Sicherungsmaßnahmen geschützt (z.H. Firewall)
- ✓ Hosting-Server werden von externen Dienstleistern Unterauftragnehmern betreut
- ✓ Ein Wartungszugriff via VPN auf externe Systeme kann durch Unterauftragnehmern erfolgen

1.4. Maßnahmen zur Sicherung von Papier-Unterlagen, mobilen Datenträgern / Endgeräten

- ✓ Nicht mehr benötigte Unterlagen mit personenbezogenen Daten werden in verschlossenen Datentonnen verwahrt. Diese werden von einem Entsorgungsdienstleister so datenschutzkonformen Vernichtung abgeholt
- ✓ Die Verwendung privater Datenträger im Unternehmen ist untersagt
- ✓ „Bring your own device“ ist im Unternehmen nicht zulässig

1.5. Maßnahmen zur sicheren Datenübertragung

- ✓ Daten werden via SSH-Key und SFTP sicher übertragen
- ✓ Schlüssel und Zertifikate werden von der Serveradministration verwaltet
- ✓ Protokolldaten werden bei Auffälligkeiten ausgewertet

Maßnahmen zur Sicherstellung der Verfügbarkeit

2.1. Serverraum

- ✓ Der Server (extern) ist Bestandteil eines durch einen externen Dienstleister betriebenen Rechenzentrums und durch die entsprechenden Maßnahmen geschützt
- ✓ Der Server (intern) wird durch einen externen Dienstleister gehostet und durch die entsprechenden Maßnahmen geschützt

2.2. Backup- und Notfall-Konzept, Virenschutz

- ✓ Es ist ein Backupkonzept vorhanden und es werden nächtliche Backups durchgeführt. Personenbezogene Daten werden hierbei täglich gesichert, auf einem separaten Server hinterlegt und nicht physisch transportiert. Die Funktionalität wird nach Erstellung automatisch überprüft.
- ✓ Es ist ein Notfallkonzept vorhanden
- ✓ IT-Systeme Werden technisch vor Datenverlusten und unbefugten Datenzugriffen geschützt. Hierzu dienen unter anderem Software zum Logging, Virenschutz, Firewall, Spam- und Phishingfilter, Protokollierung auffälliger Ereignisse.

2.3. Netzanbindung

- ✓ Die Netzanbindung wird durch einen externen Dienstleister sichergestellt, gewartet und betreut.