PRINT LOUNGE
Datenschutz-Konzept
gemäß Art. 5 DS-GVO

Das vorliegende Datenschutzkonzept hat zum Ziel, in einer zusammenfassenden Art die datenschutzrechtlichen Aspekte in Bezug auf das Unternehmen – den Softwareanbieter – und das Produkt – die Software – 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 DS-GVO.

leadprint
web-to-print solutions

Stand September 2019
Version: 1.3

Das vorliegende Datenschutzkonzept wurde durch die Geschäftsführung (André Hausmann) genehmigt.

Datenschutzbeauftragter: Sven Rahn Datenschutz

Be.Beyond GmbH & Co KG

SITZ DER GESELLSCHAFT	hanns-martin-schleyer-straße 35 47877 willich T +49 (0) 2154 / 48 09-60 F +49 (0) 2154 / 48 09-19 info@bebeyond.de www.bebeyond.de	GESCHÄFTSFÜHRER	andré hausmann gopal nath
HANDELSREGISTER	amtsgericht krefeld hra 4635 Steuernummer: 5102/5751/0464	KOMPLEMENTÄR-GESELLSCHAFT	Be.Beyond GmbH amtsgericht krefeld hrb 8907

BE.BEYOND
WERKSTATT FÜR DIGITALE GESTALTUNG

1. Einleitung und Ziele des Datenschutzkonzepts

Die Softwarelösungen der Be.Beyond GmbH & Co. KG 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 Be.Beyond GmbH & Co. KG sich selbstverständlich bewusst und hat zahlreiche Maßnahmen unternehmen, um nicht nur den datenschutzrechtlichen Bestimmungen (bspw. der DS-GVO) gerecht zu werden, sondern ein möglichst hohes und angemessenes Schutzniveau zu bieten.

1.1. Zum Unternehmen: Die Be.Beyond GmbH & Co. KG

Die Be.Beyond GmbH & Co. KG – nachfolgend “Be.Beyond” – wurde am 29. Juli 2003 in Willich gegründet und unterstützt seitdem ihre Kunden im Bereich der konzeptionellen Entwicklung und Umsetzung von Softwarelösungen im Bereich Web-to-Print.

Um dieser verantwortungsvollen Aufgabe gewissenhaft nachzukommen, beschäftigt das Unternehmen derzeit ca. 20 Mitarbeiter am Standort Willich. Die Geschäftsführung haben aktuell André Hausmann und Falk Löffler inne. Die Komplementärgesellschaft ist die Be.Beyond GmbH (AG Krefeld, HR-B 8907).

Branche	Sonstige Softwareentwicklung
Gegenstand des Unternehmens	Konzeptionelle Entwicklung und Umsetzung von Softwarelösungen & Werbemaßnahmen

2. Dokumentation und Beschreibung des Verfahrens

Das Produkt „PRINT LOUNGE“ ist eine individuelle Shop-Plattform, welche dazu geeignet ist, Web-to-Print-Dokumente zu erstellen. 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 DS-GVO Abs. 1 (bspw. 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 DS-GVO getroffen werden müssen.

2.1. Datenschutzpolitik und Verantwortlichkeiten im Unternehmen

Verantwortliche Stelle	Be.Beyond GmbH & Co. KG Hanns-Martin-Schleyer-Straße 35 47877 D-Willich Telefon: +49 (0)2154 / 48 09 - 0 Telefax: +49 (0)2154 / 48 09 – 19
Geschäftsführung	Herr André Hausmann Herr Gopal Nath
Technische Leitung	Herr Ayhan Sert
Datenschutzbeauftragter	Herr Sven Rahn – externer Datenschutzbeauftragter – Telefon: 02161 82807 - 14 E-Mail: dsb@bebeyond.de / info@rahn-datenschutz.de
Datenschutzkoordination	Herr Stefan Bleilevens – interner Datenschutzkoordinator – Telefon: 02154 4809 - 0 Fax: 02154 4809 - 19 E-Mail: dsk@bebeyond.de

2.2. Produktbeschreibung und Zweck der Software und der Verarbeitung

Die Lead-Print PRINT LOUNGE ist eine multilinguale, webbasierte Web-to-Print-Lösung, die speziell für den B2B-Bereich zur Firmenkundenbetreuung konzipiert wurde.

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. Wie alle Lead-Print Web-to-Print-Lösungen ist auch die PRINT LOUNGE sowohl in einer SaaS- als auch Kauf-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
- ✓ Kommunikationsdaten
- ✓ Vertragsstamm- & Bestelldaten
- ✓ Kundenhistorie
- ✓ Vertragsabrechnungs- & Zahlungsdaten
- ✓ Planungs- & Steuerungsdaten
- ✓ Verbindungsdaten (IP-Adresse)
- ✓ Benutzer- & Zugangsdaten
- ✓ Bildmaterial (Inhalt durch Auftraggeberin bestimmt)

Diese Auflistung umfasst die 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
- ✓ Interessenten
- ✓ Beschäftigte
- ✓ Lieferanten
- ✓ Handelsvertreter
- ✓ Ansprechpartner
- ✓ Externe Dienstleister

2.5. Empfänger von Daten

In der Regel sehen nur die Nutzer die zur Verfügung gestellten Daten (also Endkunden und Mitarbeiter der Be.Beyond im Falle von Supportfällen).

Seitens Be.Beyond ist ein Zugriff externer Programmierer und / oder Rechenzentrumsbetreiber nicht auszuschließen. Dies findet im Rahmen von Auftragsverarbeitungen gemäß Art. 28 DS-GVO statt.

2.6. Regelfristen für die Löschung der Daten

Innerhalb der Software gelten folgende Löschfristen:

Zugangs- und Benutzerstammdaten bspw. nach einer Kündigung	Manuelle Löschung bzw. Sperrung des Systems für 4 Wochen nach 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 Drittstaaten

Be.Beyond 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 kann auf Kundenwunsch auch im Frontend mit einem eigenen SSL-Zertifikat versehen werden.

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 im Rahmen der Nutzung der Software erfasst werden gilt:

1. Die Daten fallen **nicht** unter die Kategorisierung sensibler Daten nach Art. 9 Abs. 1 DS-GVO.
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), zum Beispiel Einkommen, Sozialleistungen, Grundsteuer, Ordnungswidrigkeiten“).

2. Gemäß der 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.“).

5. 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 von der PRINT LOUNGE genutzten Daten allein aus dem geschäftlichen bzw. beruflichen Umfeld stammen. Betroffen ist ausschließlich die Sozialsphäre. Der datenschutzrechtlich erforderliche Schutzbedarf ist also als „niedrig“ einzuschätzen.

3. Allgemeine Maßnahmen zum Datenschutz

Die wirksame Einhaltung der datenschutzrechtlichen Bestimmungen und insbesondere der DS-GVO erfordert eine Reihe konkreter Maßnahmen wie die folgenden Punkte aufzeigen.

3.1. Bestellung eines Datenschutzbeauftragten

Be.Beyond ist nach § 38 BDSG zur Bestellung eines Datenschutzbeauftragten verpflichtet und ist dieser Pflicht durch die Bestellung eines externen Datenschutzbeauftragten nachgekommen:

Herr Sven Rahn
– externer Datenschutzbeauftragter –

Sophienstraße 35
41065 D-Mönchengladbach

Telefon: 02161 82807 - 14
E-Mail: info@rahn-datenschutz.de

Sven Rahn ist ausgebildeter IT-Systemelektroniker. Im Jahr 2015 nahm er an einer ersten Schulung zum Datenschutzbeauftragten teil. Er ist seit 2016 hauptberuflich als externer Datenschutzbeauftragter tätig. Die geforderte Zuverlässigkeit und Fachkunde ist gegeben.

3.2. Verpflichtungserklärung der Mitarbeiter auf die Vertraulichkeit

Alle Mitarbeiter haben – in Anlehnung an die Anforderung bezüglich der Vertraulichkeit aus Art. 5 Abs. 1 lit. f DS-GVO, Art. 29 DS-GVO sowie 32 DS-GVO – eine diesbezügliche Verpflichtungserklärung unterzeichnet.

3.3. 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 8 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 korrekten und datenschutzkonformen Umgang mit der Unternehmens-EDV (und ggf. vorhandenen Papierunterlagen) geschult werden. Hierzu wird aktuell eine entsprechende, unternehmensübergreifende EDV-Nutzungsvereinbarung erarbeitet um zusätzlich zu den regelmäßigen Schulungen allen Mitarbeitern ein entsprechendes Leitbild an die Hand zu geben.

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

Be.Beyond setzt ausschließlich geprüfte, aktuelle Markengeräte (bspw. Apple, Lenovo, Samsung, BenQ, Acer) ein. Für das Dokumentenmanagement werden Produkte der Atlassian Suite eingesetzt wie beispielsweise JIRA (Projektmanagement), HipChat (interne Kommunikation – keine personenbezogenen Daten oder Zugänge, insbesondere zu Systemen mit Zugang zu personenbezogenen Daten) oder BitBucket. 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 Auslagerungen finden im Rahmen von Auftragsverarbeitungen gemäß Art. 28 DS-GVO statt. Die Unter-Auftragnehmer sind entsprechend schriftlich verpflichtet.

Server-Betrieb durch die Host Europe GmbH oder Hostway Deutschland GmbH

Die SaaS-lizensierte Software (Multimandantensystem) 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- und ggfs. Software gewährleistet. Somit ist die Software im Regelfall rund um die Uhr sicher verfügbar.

Support-Unterstützung durch externe EDV-Fachkräfte (Herr Bitsch)

Sofern die Nutzer die Software auf einem eigenen Server betreiben möchten, wird die Einrichtung, Überwachung und Koordination unter Umständen an EDV-Spezialisten in Deutschland weitergeleitet. Diese Spezialisten arbeiten langjährig und intensiv mit der Be.Beyond GmbH & Co. KG und insbesondere der Software „PRINT LOUNGE“ zusammen und liefern somit einen qualitativ hochwertigen Support.

4. Technische und organisatorische Maßnahmen

Die vollständigen und aktuellen technischen und organisatorischen Maßnahmen können jederzeit bei dem Unternehmen angefragt werden.

Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität

1.1 Zutrittskontrollmaßnahmen zu Serverräumen

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

1.2 Zutrittskontrollmaßnahmen zu Büroräumen

- ✓ Die Büroräume befinden sich in an der Hanns-Martin-Schleyer-Straße 35 in Willich
- ✓ Der Zutritt zum Gebäude und den Büroräumen ist mit einem elektronischen Schließsystem gesichert. Die Kommunikation erfolgt via RFID. Zutritt werden im System protokolliert und können bei Bedarf ausgewertet werden.
- ✓ Zutrittsrechte werden personifiziert vergeben und können jederzeit widerrufen werden.
- ✓ Betriebsfremde Personen werden am Eingang vom jeweiligen Ansprechpartner abgeholt.

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 Passwortrichtlinien im Unternehmen festgelegt.
- ✓ Bildschirme werden bei Inaktivität automatisch gesperrt oder ausgeschaltet.
- ✓ Bei Verlust eines Zugangs werden Passwörter von der Administration neu vergeben.
- ✓ Fernzugriffe 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 Sicherheitsmaßnahmen geschützt (bspw. Firewall)
- ✓ Hosting-Server werden von externen Dienstleistern (Unterauftragnehmern) betreut.

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

- ✓ Nicht mehr benötigte Unterlagen mit personenbezogenen Daten werden in verschlossenen Datentonnen verwahrt. Diese werden von einem Entsorgungsdienstleister zur 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 ist Bestandteil eines durch einen externen Dienstleister betriebenen Rechenzentrums 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.