Allgemeines zum Datenschutz

Hat LITTLE BIRD einen Datenschutzbeauftragten bestellt?

Bei der Beratung in Datenschutzfragen sowie Unterstützung als betrieblicher Datenschutzbeauftragter setzen wir auf die Dienste der Bitkom Servicegesellschaft mbH, einem der führenden Beratungsunternehmen in Deutschland rundum alle Themen der Digitalwirtschaft:
Bitkom Servicegesellschaft mbH, Albrechtstraße 10, 10117 Berlin.

Sofern Sie Fragen zum Thema Datenschutz haben, wenden Sie sich bitte an datenschutz@little-bird.de.

Wie stellt LITTLE BIRD sicher, dass mit der Auftragsverarbeitung betraute Mitarbeiter mit den gesetzlichen Bestimmungen zum Datenschutz vertraut sind?

Zum einen werden alle Mitarbeiter bei der LITTLE BIRD GmbH auf Vertraulichkeit bzw. den Datenschutz im Allgemeinen verpflichtet und mit den entsprechenden Konsequenzen im Falle eines Verstoßes vertraut gemacht.

Darüber hinaus werden regelmäßige Schulungen und Sensibilisierungsmaßnahmen zum Umgang mit personenbezogenen Daten und Datenschutz durchgeführt und dabei auch auf gesetzliche Neuerungen wie die EU Datenschutz-Grundverordnung (EU-DSGVO) eingegangen.

Was unternimmt LITTLE BIRD auf organisatorischer Ebene noch, um den Schutz der personenbezogenen Daten und die Sicherheit der IT-Systeme zu gewährleisten?

Die LITTLE BIRD GmbH orientiert sich organisatorisch an den Vorgaben der ISO/IEC 27001 und strebt die kontinuierliche Verbesserung der Prozesse und Strukturen im Datenschutz und der Informationssicherheit an. Des Weiteren arbeitet LITTLE BIRD eng mit wesentlichen Entscheidungsträgern und Gremien im Datenschutz und der IT-Sicherheit zusammen und ist unter anderem Mitglied der Gesellschaft für Datenschutz und Datensicherheit e.V., der Allianz für Cybersicherheit und des Bitkom e.V.

Wer kann einen Auftragsverarbeitungsvertrag (AV-Vertrag mit LITTLE BIRD) schließen?

Grundsätzlich sind unsere Kunden als verantwortliche Stelle als auch wir als Auftragsverarbeiter nach Art. 28 EU-DSGVO dazu verpflichtet, einen entsprechenden Vertrag zu schließen. Wir haben dazu eine entsprechende Vorlage entwickelt, welche wir Ihnen bei Vertragsschluss zukommen lassen. Auch freie und kirchliche Träger der öffentlichen Jugendhilfe können mit uns zusätzlich einen AV-Vertrag abschließen..

Was passiert, wenn es zu einer Datenpanne bei LITTLE BIRD kommt?

Sollte es wider Erwarten zu einer Datenpanne bei LITTLE BIRD Anwendung kommen, bei der personenbezogene Daten eines Kunden betroffen sind, werden wir entsprechend der gesetzlichen und vertraglichen Verpflichtungen diesen Vorfall unverzüglich dem betroffenen Kunden mitteilen, sodass dieser seinen gesetzlichen Mitteilungspflichten an die Aufsichtsbehörde und die Betroffenen nachkommen kann. Parallel informieren wir unseren externen Datenschützer zur weiteren Vorgehensweise.

Ist die Anwendung nach den Maßgaben zum Datenschutz durch Technikgestaltung entwickelt und datenschutzfreundlich voreingestellt?

Ja, Datenschutz ist integraler Bestandteil unserer Produktstrategie und damit achten wir bei der Entwicklung unserer Features bereits auf Prinzipien wie Datensparsamkeit sowie den Einsatz von Maßnahmen nach dem Stand der Technik zur Sicherstellung eines angemessenen Schutzniveaus. Im Rahmen der Vorbereitungen auf die EU-DSGVO haben wir zudem die gesamte Anwendung hinsichtlich der Voreinstellungen überprüft und soweit angepasst, dass sie ein höchstmögliches Niveau an Datenschutzfreundlichkeit bei gleichzeitiger Nutzerfreundlichkeit erreicht. Zudem sind die Einstellungen grundsätzlich so konzipiert, dass der Kunde sie nach seinen Bedürfnissen anpassen kann. Für weitere Ausführungen fordern Sie unsere technische Verfahrensbeschreibung an.

Ist die Anwendung konform nach der EU Datenschutz-Grundverordnung (EU-DSGVO)?

Die LITTLE BIRD GmbH erfüllt alle Anforderungen der EU-Datenschutz-Grundverordnung und ist als Organisation sowie als Software datenschutzkonform gemäß EU-DSGVO. Dazu haben wir im Rahmen der Vorbereitungen auf die EU-DSGVO unser Produkt auf die wesentlichen gesetzlichen Anforderungen wie Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 EU-DSGVO) oder auch die Unterstützung des Kunden bei der Wahrung der Betroffenenrechte wie Recht auf Löschung, Auskunftsrecht oder Recht auf Datenübertragbarkeit (Kapitel 3 EU-DSGVO) überprüft und entsprechende Anpassungen vorgenommen. So kann der Kunde Daten eigenverantwortlich entsprechend der gesetzlichen Vorgaben löschen. Für weiterführende Informationen fordern Sie unser „Löschkonzept“ an.

Verschlüsselung und Pseudonomisierung

Werden Kundendaten verschlüsselt gespeichert?

Ja, auf allen von der LITTLE BIRD GmbH eingesetzten Datenbanken wird eine Verschlüsselung „at Rest“ nach dem Stand der Technik eingesetzt, sodass die Daten aus der Datenbank nur nach ordnungsgemäßer Authentifizierung am jeweiligen Datenbank-System gelesen werden können.

Erfolgt die Übertragung von Kundendaten verschlüsselt?

Ja, alle personenbezogenen oder personenbeziehbaren Daten, die von der LITTLE BIRD-Anwendung an einen Client oder zu anderen Plattformen übertragen werden, müssen mittels Transport Layer Security (TLS) verschlüsselt werden, damit insbesondere auch HTTPS. Damit muss zunächst eine gesicherte Verbindung zwischen den beiden Verbindungspartnern (Client und Server) aufgebaut werden, bevor eine Datenübertragung erfolgen kann.

Vertraulichkeit und Integrität

Wo werden die Daten gespeichert?

Die LITTLE BIRD GmbHsetzt beim Hosting ihrer Software auf die Dienste der IONOS). Die genutzten Rechenzentren sind ISO/IEC 27001 zertifiziert und erfüllen somit unsere hohen Anforderungen an die physische Sicherheit der Daten unserer Kunden.

Wer kann bei LITTLE BIRD und ihren Dienstleistern auf Kundendaten zugreifen?

Grundsätzlich haben weder Mitarbeiter in den Rechenzentren noch bei AWS Zugriff auf Ihre Daten. Auf Seiten von der LITTLE BIRD Anwednung nehmen nur unser Infrastruktur Team (serverseitig) sowie unsere Produktverantwortlichen und die Mitarbeiter des Customer Success Teams (kundensystemseitig) anlassbezogen Zugriff. Die ist notwendig, um bei der initialen Einrichtung des Accounts sowie bei der Bearbeitung von Serviceanfragen zu unterstützen. Die Vergabe von Zugriffsrechten erfolgt protokolliert und nach dem “Need-to-Know”-Prinzip. Zusätzlich ist der Zugriff auf Kundensysteme protokolliert.

Wie stellt LITTLE BIRD sicher, dass keine Unbefugten Zugriff auf die Systeme des Kunden nehmen?

Do setzt serverseitig ein host-basiertes Angriffserkennungssystem zur Überwachung von Parametern wie auffälligen Log-Einträgen, Signaturen bekannter Rootkits und Trojaner, Auffälligkeiten im Device File System, oder klassischen Bruteforce-Angriffen ein. Diese Parameter werden regelmäßig auf Auffälligkeiten untersucht. Im Falle einer Auffälligkeit werden die zuständigen Mitarbeiter im Betrieb und Entwicklung sofort informiert, um Gegenmaßnahmen zu ergreifen. Zudem werden anwendungsseitig alle wesentlichen Aktivitäten (dabei insbesondere Change-, Delete-, Update-Operationen) protokolliert, um unautorisierte Zugriffe und Veränderungen an Daten auf Anfrage nachweisen zu können.

Wie erfolgt die Benutzerauthentifizierung?

Zugänge erfolgen ausschließlich über personalisierte Benutzeraccounts, die eindeutig einer Person zugeordnet sind. Die Anmeldung erfolgt mit Benutzernamen und einem Passwort, welches bei initialem Login entsprechend der in der Anwendung implementierten sicheren Passwort-Richtlinie geändert werden muss. Zusätzlichem empfehlen wir unseren Kunden die Verwendung der 2-Faktor-Authentifizierung, um ein höheres Schutzniveau zu erreichen.

In den Anmeldungen müssen Geburtsdatum und Geburtsort der Eltern angegeben werden. Können wir auf diese Daten verzichten? Wenn nein, auf welcher rechtlichen Grundlage können wir dies erheben??

Diese Erhebung basiert auf dem Grundsatz der Datenintegrität nach DSGVO : https://eu-datenschutz-grundverordnung.net/grundsaetze-fuer-die-verarbeitung-personenbezogener-daten-2/ und soll Ihre erfassten Daten innerhalb der Software eindeutig sichern, ohne das andere Datensätze aus versehen vermischt werden können. Also die Softwarelösung muss veränderungsfesten Ordnungsmerkmale sicherstellen, so dass alle Ihre Datensätze sicher und datenschutzkonform zur richtigen Person zugeordnet werden können .

Also ein Datensatz „Thomas Müller“ allein ohne Alles oder nur mit Adresse kann dazu führen, dass Datenbestände verwechselt werden, da es in Großstädten ja auch bis zu 300 Bewohner in der gleichen Adresse geben kann. Mit dem Geburtsort ist es schon wesentlich besser, da die Menge kleiner wird. Aber am Beispiel Berlin oder Köln wird deutlich, dass mehrere Thomas Müller bestimmt auch einen gleichen Geburtsort haben können es hier noch mehr Datensätze geben kann. Noch schlimmer wird es bei ausländischen Namenssätzen, da oft Väter und Söhne den gleichen Vornamen tragen. Daher das weitere Merkmal Geburtsdatum, damit die Software die geforderte Datenintegrität sicherstellt. Hier kann mit sehr hoher Wahrscheinlichkeit eine sichere Datenbankzuordnung und Einhaltung der 7 Verarbeitungsgrundsätze gewährleistet werden.

Verfügbarkeit und Belastbarkeit

Welche Mechanismen setzt die LITTLE BIRD GmbH ein, um die Verfügbarkeit zu gewährleisten?

Die LITTLE BIRD GmbH setzt hier insbesondere auf die geo-redundante Auslegung der Server-Infrastruktur in Bezug auf Produktiv-Daten und Backups sowie die physische Sicherheit der Rechenzentren (bspw. unterbrechungsfreie Stromversorgung, Alarmanlage, Brandmeldeanlage etc.) und betreibt zudem ein kontinuierliches Kapazitätsmanagement zur Überwachung der genutzten und Verteilung notwendiger Ressourcen.

Wiederherstellbarkeit

Werden regelmäßige Backups durchgeführt oder müssen Kunden ihre Daten selbst sichern?

Die LITTLE BIRD GmbH setzt zur Gewährleistung einer angemessenen Verfügbarkeit ein Backup-Konzept für die Datenbank mit den darauf gespeicherten Daten des Auftraggebers sowie das Speichermedium mit entsprechenden gespeicherten Dokumenten nach dem Stand der Technik um. Die Backups der Datenbank-Systeme werden ausschließlich verschlüsselt gespeichert. Damit ist keine Durchführung eigener Backups durch den Kunden notwendig. Es werden regelmäßige Restore-Tests durchgeführt, um sicherzustellen, dass die Backups ordnungsgemäß gespeichert wurden und im Falle eines Falles wiederherstellbar sind.

Was geschieht mit den Kundendaten, wenn es zu einem Totalausfall unseres Systems, bspw. durch eine Naturkatastrophe oder Ähnlichem, kommt?

Im unwahrscheinlichen Fall eines Totalausfalls des Systems ist durch die redundante Auslegung der Rechenzentren (Produktiv- und Backup-Daten) sichergestellt, dass Ihre Daten nicht verloren gehen. In diesem Falle werden wir entsprechend unseres Notfallplans/ Disaster Recovery Konzepts die schnellstmögliche Wiederherstellung sicherstellen.

Zweckbindung

Wem gehören die Daten?

Der Kunde ist und bleibt "Herr der Daten" und verantwortliche Stelle im Sinne des Art. 24 EU-DSGVO. Dies bedeutet insbesondere auch, dass der Kunde für die Wahrung der Betroffenenrechte (Kapitel 3 EU-DSGVO) verantwortlich ist. Die LITTLE BIRD GmbH ist Auftragsverarbeiter und verarbeitet Ihre Daten damit ausschließlich auf Ihre Weisung und zu den im Rahmen des Vertrags zur Auftragsverarbeitung geregelten Zwecke.

Das bedeutet konkret, dass Daten unter keinen Umständen an Dritte verkauft oder weiter gegeben werden. Davon ausgenommen ist eine Weitergabe an etwaig beauftragte Unterauftragnehmer, welche im Rahmen des Vertrags zur Auftragsverarbeitung mit unseren Kunden geregelt ist.

Darüber hinaus behalten wir uns vor, ausschließlich vollständig anonymisierte Daten, beispielsweise zu Zwecken des Testens oder der Weiterentwicklung des Produkts, zu verwenden. Eine solche Anonymisierung erfolgt ausschließlich im Rahmen der gesetzlichen Regelungen und berücksichtigt dabei den Stand der Technik sowie die Empfehlungen der Artikel-29-Datenschutzgruppe bzw. des Europäischen Datenschutzausschusses. Anonymisierte Daten bedeuten dabei, dass keinerlei Rückschluss auf Einzelpersonen oder Unternehmen gezogen werden kann. Damit besteht für unsere Kunden hierbei keinerlei Risiko.

Die LITTLE BIRD GmbH legt besonderen Wert darauf, den Datenschutz des Kunden zu wahren. Zusammen mit unserem Datenschutzbeauftragten haben wir deshalb technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung implementiert, welche wir kontinuierlich weiterentwickeln.

Verfahren zur Überprüfung der Sicherheit

Wie oft und durch wen wird die Sicherheit der Verarbeitung überprüft?

Wir führen regelmäßige Audits unserer Organisation und Produkt auf Basis der gesetzlichen Anforderungen zum Datenschutz durch. Die Ergebnisse dieser Audits nehmen wir zum Anlass, um Maßnahmen zu ergreifen, unsere Dokumentationen, Prozesse, Strukturen oder Funktionalitäten sowie technischen und organisatorischen Maßnahmen weiterzuentwickeln. Die Zusammenfassung des letztmaligen Audits finden Sie hier.

Führt die LITTLE BIRD GmbH auch Schwachstellenscans oder Penetrationstests durch?

Weiterhin führen wir regelmäßig interne Schwachstellenscans zur Überprüfung unserer Anwendung und Infrastruktur durch. Zudem beauftragen wir in regelmäßigen Abständen einen externen Dienstleister mit der Durchführung von Penetrationstests, um unsere Systeme und Anwendungen auf Fehler und Schwachstellen zu untersuchen. Da uns die Sicherheit unserer Systeme und Anwendung und die Angriffserkennung äußerst wichtig ist, setzen wir dabei auf den vom Bundesamt für Sicherheit in der Informationstechnik (BSI) – zertifizierten IT-Sicherheitsdienstleister secuvera GmbH. Die Ergebnisse des letzten Tests teilen wir gerne auf Anfrage mit Ihnen.