LITTLE BIRD®

Datenschutzkonzept

Das Datenschutzkonzept beschreibt die technische und organisatorische Umsetzung des Datenschutzes im Unternehmen.

Es dient der Information von interessierten Kreisen.

© LITTLE BIRD GmbH – Alle Rechte vorbehalten.

Stand 2018

1 Datenschutzleitlinie 2
1.1 Grundsätze 2
1.2 Verantwortung und Aufgaben 3
2. DATENSCHUTZBEAUFTRAGTE/R / SICHERHEITSBEAUFTRAGTE/R 4
3. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN 4
3.1 Datenschutzmanagement 4
3.2 Datenschutzorganisation 5
3.3 Beschäftigtendatenschutz 5
3.4 Datensicherheit beim Umgang mit IT Systemen 5
3.5 Berechtigungssteuerung (Zugriffskontrolle) 6
3.6 Kryptographie 6
3.7 Physische und umgebungsbezogene Sicherheit (Zutrittskontrolle) 6
3.8 Sicherer IT Betrieb 7
3.9 Kommunikationssicherheit 8
3.10 Anschaffung, Entwicklung und Instandhaltung von IT Systemen 8
3.11 Lieferantenbeziehungen/ Auftragsdatenverarbeiter 8
3.12 Handhabung von Datenschutzvorfällen 9
3.13 Business Continuity Management und Verhalten bei Datenschutznotfäl-len 9
3.14 Weitere Datenschutz-Compliance Maßnahmen 9
4. WEITERE MASSNAHMEN 10
4.1 Verzeichnisse von Verarbeitungstätigkeiten 10
4.2 Datenschutz-Folgeabschätzungen 10
4.3 Schulung und Sensibilisierung der MitarbeiterInnen 10
5. Regelungen im Unternehmen 10

© 2018 LITTLE BIRD GmbH – Alle Rechte vorbehalten.

1 Datenschutzleitlinie

Der Schutz der in unserem Unternehmen verarbeiteten personenbezogenen Daten, insbesondere die Wahrung ihrer Vertraulichkeit, Integrität und Verfügbarkeit, ist unsere Pflicht und wird von den bereits genannten Kreisen ggf. auch kontrolliert.

Aufgrund der möglichen drastischen Bußgelder kann die Verletzung von Datenschutzvorschriften ohne weitere Voraussetzungen für das Unternehmen existenzbedrohende Auswirkungen haben.

Die Geschäftsführung ist sich der hohen Bedeutung des Datenschutzes und seiner persönlichen Verantwortlichkeit bewusst. Mit der Einführung, Umsetzung und stetigen Verbesserung des DSMS wollen wir den hohen Stellenwert unterstreichen, den die Verarbeitung personenbezogener Daten für uns hat.

1.1 Grundsätze

Die Erfüllung der gesetzlichen Anforderungen stellt das Mindestmaß unserer Datenschutzbemühungen dar. Zur Erfüllung gesetzlicher Pflichten erforderliche Maßnahmen müssen mit Priorität umgesetzt werden.

Alle Maßnahmen haben sich daran zu orientieren, ob sich mit einem verhältnismäßigen Einsatz von Mitteln ihr Ziel erreichen lässt. Ziel ist stets, die mit einer Verarbeitung einhergehenden Risiken angemessen zu beherrschen, möglichst aber, ohne die eigenen Interessen des Unternehmens über Gebühr einzuschränken.

Für die Verarbeitung personenbezogener Daten gelten die folgenden Grundsätze:

Wir verarbeiten personenbezogene Daten nur, wenn und solange dafür eine klare Erlaubnis oder Verpflichtung besteht!

Der jeweils konkret verfolgte Zweck einer Verarbeitung und die hierfür beanspruchte Rechtsgrundlage werden im Verzeichnis der Verarbeitungstätigkeiten dokumentiert. Eine hier nicht behandelte Verarbeitung von Daten darf nicht erfolgen!

Wir vermeiden personenbezogene Daten!

Es werden nur insoweit Daten eingesetzt, wie dies zur Erreichung eines legitimen Zwecks erforderlich ist. Zur Erreichung eines bestimmten Zwecks nicht relevante Daten werden nicht verarbeitet.

Soweit sich ein Zweck auch mit anonymen oder pseudonymen Daten angemessen erreichen lässt, müssen diese verwendet werden. Entsprechend geht auch die Verarbeitung allgemeiner oder verallgemeinerter Informationen der Verarbeitung von Detailinformationen vor.

Auch die Dauer der Verarbeitung ist auf das erforderliche Maß zu begrenzen. Daten sind – unter Beachtung etwaiger Aufbewahrungspflichten – frühestmöglich zu löschen.

Wir beachten die Interessen der Betroffenen!

Jede Verarbeitung erfolgt nur unter Berücksichtigung der Interessen und Erwartungen der Betroffenen. Personenbezogene Daten werden nur genutzt, soweit dies zur Erreichung eines legitimen Zwecks unvermeidbar und dem Betroffenen zumutbar ist.

Wir tragen dafür Sorge, dass die durch uns erfolgende Verarbeitung für den Betroffenen nachvollziehbar ist und achten die Rechte der Betroffenen, insbesondere auf Information.

Wir handhaben den Zugriff auf personenbezogene Daten restriktiv!

Wir behandeln alle personenbezogenen Daten streng vertraulich! Daten werden Personen oder Prozessen nur zugänglich gemacht, wenn, soweit und solange dies im Einzelfall notwendig ist. Diese Beschränkung gilt sowohl für Datensammlungen insgesamt, als auch für die darin enthaltenen Detailinformationen.

© 2018 LITTLE BIRD GmbH – Alle Rechte vorbehalten.

Wir achten auf die Richtigkeit der personenbezogenen Daten, die wir verarbeiten!

Wenn wir erfahren, dass solche Daten nicht korrekt sind, berichtigen wir diese unverzüglich.

Wir sorgen für Sicherheit bei der Datenverarbeitung!

Durch dem Stand der Technik entsprechende technische und organisatorische Maßnahmen stellen wir einen angemessenen Schutz vor Datenschutzverletzungen sicher. Dabei berücksichtigen wir das Risiko, welches mit einer Verarbeitung verbunden ist.

Wir können unsere Datenschutzbemühungen nachweisen!

Wir beurteilen und messen den Erfolg unserer Datenschutzmaßnahmen in angemessenem Umfang und korrigieren Fehlentwicklungen.

1.2 Verantwortung und Aufgaben

Die Geschäftsführung trägt zwar rechtlich die Gesamtverantwortung für den Datenschutz, kann aber die zu bewältigenden Aufgaben tatsächlich nicht allein erledigen. Der Aufbau einer geeigneten Organisation und die Delegation von Aufgaben sind damit notwendig und Pflicht der Geschäftsführung. Die Geschäftsführung bleibt für die korrekte Auswahl und Überwachung der eingesetzten MitarbeiterInnen persönlich verantwortlich.

Die Geschäftsführung kann ihrer verbleibenden Verantwortung nur gerecht werden, wenn sie angemessen informiert ist. Daher ist ein entsprechendes Berichtswesen einzurichten. Alle Verantwortlichen haben das Recht, direkt an die Geschäftsführung zu berichten.

Grundsätzlich sind alle MitarbeiterInnen aufgerufen, die Datenschutzbemühungen des Unternehmens aktiv zu unterstützen und in ihrem Aufgabenbereich nach besten Kräften für die korrekte Umsetzung von Vorgaben zu sorgen. Sie werden entsprechend geschult und laufend sensibilisiert. Mitarbeiter sind angemessen anzuleiten. Alle Mitarbeiter sind insoweit auch persönlich verantwortlich.

Für alle Bereiche oder Aufgaben ist eindeutig festzulegen, wem die Verantwortung übertragen wird. Die Zuweisung erfolgt immer an eine bestimmte Person, die auch über ihre Funktion oder Rolle benannt werden kann. Soweit erforderlich, sind geeignete StellvertreterInnen zu benennen. VertreterInnen können auch mehrere Personen oder Angehörige einer Rolle sein. Es ist stets scherzustellen, dass der / die Verantwortliche und VertreterIn sowohl fachlich als auch persönlich in der Lage sind, ihre Aufgaben sorgfältig, vertrauensvoll und angemessen zu erfüllen.

Bei der Zuweisung von Verantwortlichkeiten müssen Interessenskonflikten vermieden werden. Miteinander unverträgliche Rollen sind zu bestimmen und zu dokumentieren.

Über die Verantwortlichkeiten im Unternehmen wird eine laufende Dokumentation geführt.

Um zu gewährleisten, dass relevante Interessen auch bereichsübergreifend berücksichtigt werden, ist bei der Konzeption eines Prozesses festzulegen, welche Rollen, Stellen oder Personen ggf. zu beteiligen oder zu informieren sind.

Folgende Rollen haben besondere Aufgaben im Bereich des Datenschutzes:

- **Datenschutzbeauftragte/r:** Der / Die Beauftragte für den Datenschutz unterrichtet und berät die Angehörigen des Unternehmens hinsichtlich ihrer datenschutzrechtlichen Verpflichtungen. Er überwacht die Einhaltung der Datenschutzvorschriften. Der / Die Beauftragte ist keinen Weisungen unterworfen und nicht für die korrekte Umsetzung des Datenschutzes verantwortlich. Die Pflicht zur Bestellung eines / einer Datenschutzbeauftragten richtet sich nach dem Gesetz.
- **Datenschutzverantwortliche/r:** Die rechtliche Verantwortung für die Beachtung des Daten-schutzes trägt stets die Geschäftsführung. Bei mehreren Personen muss klargestellt werden, ob die Verantwortung gemeinsam ausgeübt wird, oder ob die Aufgaben einem Ange-

© 2018 LITTLE BIRD GmbH – Alle Rechte vorbehalten.

hörigen der Geschäftsführung übertragen wurde. Die Umsetzung der von der Geschäfts-führung initiierten Maßnahmen kann auch an andere Personen delegiert werden.

- **DatenschutzkoordinatorIn:** Bei Übertragung der Verantwortung von der Geschäftsführung auf eine andere Person muss eindeutig bestimmt sein, wem die Verantwortung für die Um-setzung des Datenschutzes zugewiesen wurde. Auch muss in diesen Fällen der / die DatenschutzkoordinatorIn mit den erforderlichen Weisungsbefugnissen ausgestattet werden. Der / Die eingesetzte KoordinatorIn trägt Sorge für die Umsetzung des Datenschutzes in den einzelnen Abteilungen des Unternehmens und er stellt ggf. die Abstimmung zwischen diesen her. Der / Die KoordinatorIn berichtet der Geschäftsführung.

2. DATENSCHUTZBEAUFTRAGTE/R / SICHERHEITSBEAUFTRAGTE/R

Kontakt zum externen Datenschutzbeauftragten:

Raphael Hoffmann

hoffmann@activemind.de

+49 (0)30 / 770 19 10 70

3. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Nachstehend wird beschrieben, welche technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt sind. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Unternehmen verarbeiteten Informationen. Die Struktur orientiert sich nach der international anerkannten Norm DIN ISO/IEC 27002.

3.1 Datenschutzmanagement

Die Datenschutzleitlinie der LITTLE BIRD GmbH beinhaltet die Leitaussagen der Geschäftsleitung zum Umgang mit personenbezogenen Daten im Unternehmen. Zusätzlich haben wir eine IT Sicherheitsleitlinie im Unternehmen implementiert, die die Leitaussagen des Unternehmens in Bezug auf Verfügbarkeit, Integrität und Vertraulichkeit der Daten regelt.

Alle Beschäftigten, freie MitarbeiterInnen und unterstützende Unternehmen sind verpflichtet diese zentralen Regelungen zu beachten.

Das erreichte Datenschutz- und Datensicherheitsniveau der Organisationseinheiten, Prozesse und Systeme wird durch eine Kombination aus periodisch wiederkehrenden Prüfungen und kontinuierlichen Kontrollen überwacht.

Die Überwachungen des laufenden Betriebs erfolgen in Abstimmung mit dem Datenschutz- und ggf. dem / der Sicherheitsbeauftragten.

Ein Review der Datenschutzpolitik erfolgt zumindest jährlich, soweit nicht ein Anlass für eine häufigere Überprüfung besteht. Hierdurch wird die laufende Angemessenheit, Eignung und Effektivität der Regelung sichergestellt.

Die Geschäftsführung hat die Verantwortung für den Datenschutz im Unternehmen.

© 2018 LITTLE BIRD GmbH – Alle Rechte vorbehalten.

3.2 Datenschutzorganisation

Die Führungskräfte der LITTLE BIRD GmbH sind in ihrer Organisationseinheit für die vollständige Umsetzung der Grundsätze des Datenschutzes und der Datensicherheit und für die Erfüllung der an sie gestellten Datenschutzaufgaben verantwortlich.

Rollen und -verantwortlichkeiten sind im Rahmen des Datenschutzmanagements definiert. Miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche sind getrennt, um die Möglichkeiten zu unbefugter oder unbeabsichtigter Änderung oder zum Missbrauch der Werte unseres Unternehmens zu reduzieren.

Wir verfügen über ein Verfahren, das festlegt, wann und durch wen relevante Behörden benachrichtigt und erkannte Datenschutzvorfälle rechtzeitig gemeldet werden.

In unseren Projekten ist Datenschutz und Datensicherheit Bestandteil aller Phasen unserer Projektmethodik.

Durch unsere jeweiligen Richtlinien und Prozesse zur Telearbeit und der Nutzung von Mobilgeräten, stellen wir den Datenschutz und die Datensicherheit auch in diesen Bereichen sicher.

3.3 Beschäftigtendatenschutz

Wir haben unsere MitarbeiterInnen sorgsam ausgewählt und ihre Eignung für ihre Rolle im Unternehmen überprüft. Ihre Verantwortlichkeiten haben wir in Funktionsbeschreibungen festgelegt und gleichen stetig ab, ob die MitarbeiterInnen diesen entsprechen. Vor Beginn ihrer Anstellung unterschreiben alle MitarbeiterInnen eine Vertraulichkeits- sowie Datenschutzvereinbarung, die über die Beendigung des Beschäftigungsverhältnisses hinaus gilt. Die MitarbeiterInnen werden im Bereich Datenschutz- und Datensicherheit geschult, insbesondere werden Schulungen bei Funktionswechsel noch einmal aufgefrischt. Sie sind sich daher ihrer Verantwortung diesbezüglich bewusst.

In einem dokumentierten Prozess für die Zeit vor, während und nach Beendigung des Beschäftigungsverhältnisses stellen wir sicher, dass personenbezogene Daten geschützt und die Datensicherheit gewährleistet ist. Diese beinhaltet auch Maßregelungen für den Fall eines Datenschutzverstoßes.

3.4 Datensicherheit beim Umgang mit IT Systemen

Sämtliche Werte (wie z.B. Betriebsmittel, Wechseldatenträger, Notebooks) und Informationen, die mit personenbezogenen Daten in Zusammenhang stehen, werden von uns inventarisiert und gepflegt.

Wir haben zum Schutz dieser Werte Verantwortliche festgelegt, die für den Lebenszyklus eines Wertes zuständig sind.

Es wurden dokumentierte Regeln für den zulässigen Gebrauch unserer Werte aufgestellt. Die Rückgabe erfolgt dokumentiert.

Nicht mehr benötigte Datenträger entsorgen wir sicher, unter Anwendung eines dokumentierten Verfahrens und verpflichteter zertifizierter Dienstleister.

© 2018 LITTLE BIRD GmbH – Alle Rechte vorbehalten.

3.5 Berechtigungssteuerung (Zugriffskontrolle)

Wir verfügen über geregelte und dokumentierte Maßnahmen, die sicherstellen, dass berechtigte Personen nur auf solche personenbezogenen Daten Zugriff erhalten, für die sie die Befugnis zur Einsichtnahme und zur Verarbeitung besitzen.

Berechtigungen zum Zugriff auf IT-Systeme werden über ein geregeltes Verfahren auf der Grundlage eines dokumentierten und restriktiven Berechtigungskonzepts vergeben. Den Zugang zu Netzwerken und Netzwerkdiensten haben wir geregelt und umgesetzt.

Es ist sichergestellt, dass nur befugte Benutzer Zugang zu Systemen und Diensten haben und unbefugter Zugang unterbunden wird, insbesondere besteht ein formaler Prozess für die Registrierung und Deregistrierung von Benutzern, der die Zuordnung von Zugangsrechten zu ermöglicht.

Unsere administrativen Rechte erteilen wir eingeschränkt und gesteuert.

Wir verfügen über einen dokumentierten und geregelten Prozess über den Umgang mit Passwörtern.

Ist- und Soll-Zustand von Benutzerzugangsrechten werden stetig abgeglichen. Bei Bedarf werden diese entzogen oder angepasst.

Wir schränken den Zugriff auf unsere Daten bedarfsgerecht ein und steuern den Zugang auf unsere Systeme und Anwendungen durch ein sicheres Anmeldeverfahren. Wir verwenden ein System zur Nutzung sicherer und starker Kennwörter.

Der Gebrauch von Hilfsprogrammen, die fähig sein könnten, System- und Anwendungsschutzmaßnahmen zu umgehen, ist eingeschränkt und streng überwacht.

3.6 Kryptographie

Der angemessene und wirksame Gebrauch von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Information und personenbezogenen Daten ist sichergestellt. Zu diesem Zwecke haben wir eine Richtlinie über den Einsatz von Kryptographischen Maßnahmen im Unternehmen implementiert, die auch die Verwaltung von kryptographischen Schlüsseln umfasst und dem Schutzbedarf angemessen ist.

3.7 Physische und umgebungsbezogene Sicherheit (Zutrittskontrolle)

Wir haben dokumentierte und geregelte Maßnahmen getroffen, die verhindern sollen, dass Unbefugte Zutritt zu Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet oder genutzt werden. Diese umfassen unter anderem:

- Die Geschäftsräume liegen im xxx eines Bürogebäudes und werden exklusiv genutzt.
- Der zentrale Eingang wird überwacht.
- Türen zu Sicherheitsbereichen sind stets geschlossen. Schutz erfolgt über ein Token basiertes System
- Besucher oder externe Dienstleister werden individuell eingelassen.
- Der Brandschutz wird beachtet
- Es sind Sicherheitsbereiche vorhanden, zu denen nur eigens hierzu Berechtigte Zutritt erhalten.
- IT-Räume sind separat verschlossen und nur durch Berechtigte zu öffnen.
- Versorgungseinrichtungen werden vor Stromausfällen und Störungen geschützt
- Die Sicherheit der Verkabelung wird beachtet
- Die Instandhaltung von Systemen wird geplant und umgesetzt

© 2018 LITTLE BIRD GmbH – Alle Rechte vorbehalten.

- Das Entfernen und Änderungen von Systemen und Informationen erfolgt geregelt.
- Die Sicherheit von Systemen außerhalb der Geschäftsräume wird beachtet.
- Die Entsorgung oder Wiederverwendung von Betriebsmitteln erfolgt geregelt
- Richtlinien für Clean Desk und Bildschirmsperren werden umgesetzt.

3.8 Sicherer IT Betrieb

Wir verfügen über geregelte und dokumentierte Maßnahmen, um einen ordnungsgemäßen und sicheren Betrieb von informations- und datenverarbeitenden Einrichtungen sicherzustellen. Diese umfassen u.a. die Steuerung im Falle einer Änderung an den informationsverarbeitenden Einrichtungen, als auch eine Steuerung und stetige Messung unserer Kapazitäten und Ressourcen, um die Verfügbarkeit der erforderlichen Systemleistung sicherzustellen. So werden z.B. unteranderem folgende Werte laufend aktuell überwacht:

- Festplattenstatus und verfügbarer Speicher
- Raid-Status
- Dienste und Status aller virtuellen Maschinen
- Speicherbelegung der Storages und Hauptspeicher
- Auslastung Ethernet in Kbit/s und Mbit/s
- Durchsatz und Auslastung der Firewall
- Erreichbarkeit aller Server von außen

Ein geschütztes Verfahren zur Datensicherung wurde von uns implementiert und ist dokumentiert.

Standardwartungsfenster sind definiert. Zusätzlich notwendige Fenster werden mindestens 10 Tage vorab angekündigt.

In unserem Unternehmen ist es essentiell, Entwicklungs-, Test und Betriebsumgebungen voneinander zu trennen, so dass wir ein besonderes Augenmerk hierauf haben.

Maßnahmen zur Erkennung, Vorbeugung und Wiederherstellung zum Schutz von Schadsoftware wurden getroffen und werden stetig aktualisiert.

Wir verfügen über eine zentral überwachte und geschützte Ereignisprotokollierung und haben für den Fall der Speicherung sensibler personenbezogener Daten Maßnahmen zum Schutz der Privatsphäre getroffen. Sämtliche Protokollierungseinrichtungen und Protokollinformationen, einschließlich Administratoren und Bedienerprotokolle sind vor Manipulation und unbefugtem Zugriff geschützt.

Die Synchronisation unserer Uhren erfolgt zentral mit einer einzigen Referenzzeitquelle.

Wir verfügen über ein zentrales Verfahren zur gesteuerten Installation von Software auf Systemen in unserem Unternehmen.

Es besteht eine Aufstellung unserer technischen Werte und eine geregelte, dokumentierte Handhabung für den Fall einer technischen Schwachstelle, die u.a. unser Patchmanagement mit definierten Verantwortlichkeiten umfasst.

Regelungen für die Einschränkungen von Softwareinstallationen sind von uns zentral implementiert.

Im Falle einer Auditprüfung unserer Informationssysteme haben wir Maßnahmen festgelegt, die Störungen der Geschäftsprozesse soweit wie möglich minimieren.

© 2018 LITTLE BIRD GmbH – Alle Rechte vorbehalten.

3.9 Kommunikationssicherheit

Die Sicherheit unserer in Netzwerken und Netzwerkdiensten gespeicherten personenbezogenen Daten und Informationen ist unumgänglich. Daher haben wir dokumentierte Maßnahmen eingesetzt, die unsere Netzwerke verwalten, steuern und sichern.

Informationsdienste, Benutzer und Informationssysteme werden bedarfsgerecht voneinander getrennt gehalten.

Wir verfügen über Richtlinien und Verfahren für die Informations- und Datenübertragung, sowie die Vereinbarungen zur Datensicherheit an externe Stellen.

Unsere elektronische Nachrichtenübermittlung wird angemessen geschützt. So haben wir unter anderem Maßnahmen zum Schutz der Nachrichten vor unbefugtem Zugriff, vor Veränderung oder Denial of Service getroffen, die dem von der Organisation übernommenen Klassifizierungsschema entsprechen.

Um unsere Daten zu schützen, schließen wir bedarfsgerechte Vertraulichkeits- oder Geheimhaltungs-vereinbarungen ab, die wir stetig überprüfen.

3.10 Anschaffung, Entwicklung und Instandhaltung von IT Systemen

Es ist sichergestellt, dass Daten- und Datensicherheit ein fester Bestandteil über den gesamten Lebenszyklus unserer Systeme ist. Dies beinhaltet auch die Anforderungen an und die Sicherung von Informationssystemen, die Dienste über öffentliche Netze bereitstellen. Der Schutz der Transaktionen bei Anwendungsdiensten erfolgt bedarfsgerecht. Zudem haben wir ein Verfahren zur Verwaltung von Systemänderungen eingerichtet, um die Integrität des Systems, der Anwendungen und der Produkte von den frühen Entwurfsphasen bis zu allen später anfallenden Wartungsarbeiten sicherzustellen. Bei Änderungen an Betriebsplattformen werden geschäftskritische Anwendungen überprüft und getestet, um sicherzustellen, dass es keine negativen Auswirkungen auf die Organisationssicherheit auch der Kundenanwendungen gibt. Wir verfügen über einen gesteuerten Prozess zur Analyse, der Entwicklung und der Pflege sicherer IT Systeme.

Für neue Informationssysteme, Aktualisierungen und neue Versionen sind Abnahmetestprogramme und dazugehörige Kriterien festgelegt. Unsere Testdaten werden sorgfältig ausgewählt geschützt und gesteuert.

3.11 Lieferantenbeziehungen/ Auftragsdatenverarbeiter

Wir wählen unsere Lieferanten im Vorfeld sorgsam aus und überprüfen ihre Geeignetheit hinsichtlich der Wahrung des Datenschutzes und der Datensicherheit.

Dokumentierte Vereinbarungen sichern den Schutz und die Geheimhaltung unserer Werte und Daten. Im Falle einer Auftragsdatenverarbeitung werden Auftragsverabeitungsverträge mit den Lieferanten abgeschlossen. Die Lieferanten werden verpflichtet, technisch-organisatorische Maß-nahmen zu treffen, um dies zu gewährleisten.

Es besteht eine reglementierte und benutzerdefinierte Zugriffsberechtigung auf die für den jeweiligen Lieferanten zwingend benötigten Werte und Daten.

Lieferanten dürfen weitere Lieferanten lediglich mit unserer Zustimmung beauftragen, um eine sichere Lieferkette zu gewährleisten.

© 2018 LITTLE BIRD GmbH – Alle Rechte vorbehalten.

Stetig führen wir eine Überprüfung der Datenschutz- und Datensicherheitsmaßnahmen unserer Lieferanten durch, um das vereinbarte Niveau aufrecht zu erhalten. Auch die zugewiesenen Berechtigungen unterliegen einer ständigen dokumentierten Kontrolle.

Nach Beendigung des Lieferantenverhältnisses sind diese verpflichtet, die von uns erhaltenen Daten und Werte zu vernichten. Zudem gilt die Wahrung der Geheimhaltungspflicht unbegrenzt.

3.12 Handhabung von Datenschutzvorfällen

Unser Unternehmen verfügt über einen geregelten dokumentierten Prozess für die Handhabung von Datenschutzvorfällen, um diesbezüglich eine konsistente und wirksame Herangehensweise zu gewährleisten. Die MitarbeiterInnen sind angehalten, sämtliche Datenschutz – und Sicherheitsereignisse unverzüglich zu melden und werden diesbezüglich stetig geschult. Wir haben ein Meldesystem installiert, das Ereignisse an ein Interventionsteam weitergeleitet, um eine schnelle Reaktion zu gewährleisten. Sämtliche Ereignisse werden dokumentiert, klassifiziert und bewertet. Das implementierte Interventionsteam hat genaue Vorgaben, wie auf ein Ereignis zu reagieren ist.

Zusammen mit der Geschäftsführung werden stetig Verbesserungsmaßnahmen besprochen und um-gesetzt, die sich aus den Erkenntnissen und den gesammelten Beweisen eines Ereignisses ergeben.

3.13 Business Continuity Management und Verhalten bei Datenschutznotfällen

Im Rahmen des Datenschutzes und der Datensicherheit wird die vorgesehene Verfügbarkeit von Systemen eigens bewertet. Aus den Anforderungen leiten wir die technischen und organisatorischen Vorgaben, wie redundante Systeme / Anbindungen oder entsprechende Planungen ab und setzen diese konsequent und gesteuert um. Alle Server und Storage Systeme sind mit einer 36-monatigen Herstellergarantie ausgestattet.

3.14 Weitere Datenschutz-Compliance Maßnahmen

Wir haben alle relevanten gesetzlichen, regulatorischen, selbstauferlegten oder vertraglichen Anforderungen sowie das Vorgehen unseres Unternehmens zur Einhaltung dieser Anforderungen bestimmt, dokumentiert und halten diese auf dem neuesten Stand.

Die betroffenen Personen werden, wie gesetzlich gefordert, bei Erhebung ihrer personenbezogenen Daten informiert.

Auch wurden angemessene Verfahren umgesetzt, mit denen die Einhaltung gesetzlicher, regulatorischer und vertraglicher Anforderungen mit Bezug auf geistige Eigentumsrechte und der Verwendung von urheberrechtlich geschützten Softwareprodukten sichergestellt ist.

Entsprechend der gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen schützen wir Aufzeichnungen und personenbezogene Daten bedarfsgerecht. Jährliche Tätigkeitsberichte des / der Datenschutzbeauftragten dokumentieren die ergriffenen Maßnahmen.

Um den Schutz unserer personenbezogen Daten sicher zu stellen, erfolgt stetig eine unabhängige Überprüfung unseres Datensicherheits- und Datenschutzniveaus, unserer Sicherheits- und Datenschutzrichtlinien, sowie die Einhaltung von technischen Vorgaben.

© 2018 LITTLE BIRD GmbH – Alle Rechte vorbehalten.

4. WEITERE MASSNAHMEN

4.1 Verzeichnisse von Verarbeitungstätigkeiten

Aktuelle Verzeichnisse von Verarbeitungstätigkeiten sind vorhanden.

4.2 Datenschutz-Folgeabschätzungen

Soweit gesetzlich gefordert, werden Verfahren vor ihrer Inbetriebnahme auf Basis vordefinierter Risikokriterien und –stufen identifiziert und den Schutzmaßnahmen gegenübergestellt. Die so getroffenen datenschutzrechtlichen Bewertungen fließen in die Umsetzung der Maßnahmen ein und werden dokumentiert.

4.3 Schulung und Sensibilisierung der MitarbeiterInnen

MitarbeiterInnen werden stetig in Fragen des Datenschutzes und der Datensicherheit dokumentiert geschult und sensibilisiert.

5. Regelungen im Unternehmen

Es bestehen unter anderem folgende Datensicherheits- und Datenschutzregelungen im Unternehmen:

- Richtlinie Betroffenenrechte
- Richtlinie Risikoanalyse und –behandlung
- Onboarding MitarbeiterInnen
- Offboarding MitarbeiterInnen
- Richtlinie Auftragsverarbeitung
- Richtlinie Berechtigungsvergabe
- Richtlinie Datenschutznotfall
- Richtlinie Datenarchivierung und –löschung
- Richtlinie IT-Nutzung
- Kontaktpersonen im Rahmen eines Datenschutznotfalles

© 2018 LITTLE BIRD GmbH – Alle Rechte vorbehalten.