Informationssicherheits- und Datenschutzrichtlinie für Dienstleister und Lieferanten

Unternehmen
LAT GmbH
Alfred-Brehm-Str. 5
85053 Ingolstadt

Stand: 13.07.2023

Inhaltsverzeichnis

1 Vorwort (Unternehmen und Geschäftszweck)

Seit der Gründung 1993 hat die LAT GmbH das ursprüngliche Kernarbeitsgebiet der Laserbeschriftung kontinuierlich fortentwickelt. Kompetenzen und Fertigungskapazitäten wurden systematisch ausgebaut und die Geschäftsfelder schrittweise um angrenzende Technologien erweitert.

Heute nimmt die LAT GmbH im Bereich der Laserbeschriftung mit den Nachbartechnologien Werkzeugbau, Kunststoffspritzguss, Lackierung, Schilder- und Etikettenherstellung in vielen industriellen Anwendungsgebieten eine technologisch führende Rolle ein und bedient unterschiedlichste Kundenansprüche von der Planung und Projektierung bis zur bedarfsgerechten Lieferung.

Die Einführung eines strukturierten Informations-Sicherheits-Management-Systems (ISMS) gemäß TISAX und eines Business-Continuity-Management-Systems (BCMS) gemäß der ISO 22301 beruht auf einer Kundenanforderung und damit einhergehend auf einer strategischen Entscheidung der Geschäftsleitung.

2 Geltungsbereich/Anwendungsbereich

Diese Sicherheitsrichtlinie gilt für alle Dienstleister und Lieferanten, die für unser Unternehmen tätig sind und dabei Zugang zu unseren Datenverarbeitungssystemen haben oder wenn Dienstleister oder Lieferanten informationssicherheitsrelevante Informationen und Daten gemäß Ziffer 5 von unserem Unternehmen erhalten. Ein Verstoß gegen die Vorgaben zur Sicherstellung der Informationssicherheit kann Schadensersatzforderungen durch das Unternehmen oder durch Kunden zur Folge haben.

3 Einhaltung von Rechtsvorschriften

Bei Umgang mit Informationen in unserem Unternehmen sind von den Dienstleistern und Lieferanten die geltenden Rechtsvorschriften zu Datenschutz (DS-GVO und BDSG) und Informationssicherheit (VDA-ISA) sowie unsere Unternehmensregelungen einzuhalten. Sollten Dienstleister und Lieferanten unsicher sein, ob und inwieweit Rechtsvorschriften oder Unternehmensregelungen einzuhalten sind, haben sie sich an unseren Informationssicherheitsbeauftragten oder ihren Ansprechpartner in unserem Unternehmen zur Klärung zu wenden.

4 Abweichen von Vorgaben

Jegliche Abweichung von den Informationssicherheitsvorgaben dieser Richtlinie bedarf der vorherigen dokumentierten Freigabe durch den Informationssicherheitsbeauftragten. Hierbei ist ggfs. der Datenschutzbeauftragte in die Entscheidungsfindung mit einzubeziehen, sofern es sich um eine datenschutzrelevante Abweichung handelt.

5 Arten von Informationen

Zur Gewährleistung des sicheren und sorgsamen Umgangs mit Informationen sind die folgenden 4 Kategorien für die Einstufung von Informationen hinsichtlich Vertraulichkeit festgelegt.

5.1 Geheime Informationen

- Die Einstufung **geheim** bezeichnet die vertraulichsten aller Informationen gemäß Schutzklasse 3 der DIN 66399 und der Sicherheitsstufen 4, 5, 6 und 7. Die Weitergabe von geheimen Informationen muss auf einen sehr kleinen, namentlich bekannten Kreis von Personen beschränkt sein.
- Geheime Informationen sind immer unter Verschluss zu halten.
- Papierunterlagen sind mit dem Wort „geheim“ zu kennzeichnen, dies kann durch einen Stempel oder ähnliche Kennzeichnungen erfolgen.
- Für die Erstellung von geheimen Informationen ist eine spezielle Vorlage (mit Fußzeile „geheim“) zu verwenden.
- Geheime Informationen dürfen nur inhaltsverschlüsselt per E-Mail versendet werden.

- Das Speichern von geheimen Informationen darf auf mobilen Datenträgern nur verschlüsselt erfolgen, wenden Sie sich im Bedarfsfall an die IT-Abteilung.
- Die Löschung und Vernichtung müssen in geeigneter Weise erfolgen (Aktenvernichter etc.).

Beispiele für **geheim** eingestufte Informationen sind:

- Passwörter
- Unterlagen zu neuen Entwicklungen
- Unterlagen, die von unserem Unternehmen oder von unserem Kunden als geheim klassifiziert wurden.

5.2 Vertrauliche Informationen

- Die Einstufung **vertraulich** bezeichnet Informationen mit dem zweithöchsten Vertraulichkeitsniveau gemäß Schutzklasse 2 der DIN 66399 und der Sicherheitsstufe 3. Die Weitergabe von vertraulichen Informationen muss auf einen kleinen Personenkreis beschränkt sein.
- Vertrauliche Informationen sind immer unter Verschluss zu halten.
- Papierunterlagen sind mit dem Wort „vertraulich“ zu kennzeichnen, dies kann durch einen Stempel oder ähnliche Kennzeichnungen erfolgen.
- Für die Erstellung von vertraulichen Informationen ist eine spezielle Vorlage (mit Fußzeile „vertraulich“) zu verwenden.
- Vertrauliche Informationen dürfen nur transportverschlüsselt per E-Mail versendet werden, wenden Sie sich hierzu an die IT-Abteilung.
- Das Speichern von vertraulichen Informationen darf auf mobilen Datenträgern nur verschlüsselt erfolgen, wenden Sie sich im Bedarfsfall an die IT-Abteilung**.**
- Das Speichern von vertraulichen Informationen erfolgt in Dateiverzeichnissen mit eingeschränktem Benutzerzugriff.

Beispiele für **vertraulich** eingestufte Informationen sind:

- Vertragsunterlagen
- Unterlagen, die von unserem Unternehmen oder von unserem Kunden als vertraulich klassifiziert wurden.

5.3 Interne Informationen

- **Intern** ist die gebräuchlichste Einstufung von Informationen gemäß Schutzklasse 1 der DIN 66399 und der Sicherheitsstufen 1 und 2. Die Weitergabe von internen Informationen ist normalerweise auf größere Personengruppen beschränkt. Der Versand von Emails ist unverschlüsselt möglich. Alle erstellten Dokumente gelten grundsätzlich zunächst als „intern“ und sind in der Fußzeile der erstellten Dokumente zu kennzeichnen.

Beispiele für **intern** eingestufte Informationen sind:

- Telefonverzeichnis der Mitarbeiter
- Organigramme
- Aufgabenbeschreibungen

5.4 Öffentliche Informationen

- Als **öffentlich** eingestufte Informationen sind nicht vertraulich und für den allgemeinen Gebrauch innerhalb und außerhalb des Unternehmens bestimmt.

Beispiele für **öffentlich** eingestufte Informationen sind:

- Marketingunterlagen
- Vertriebspräsentationen
- Referenzlisten

Die Verantwortung für die richtige Klassifizierung und dem Umgang mit den Informationen trägt der Informationseigner.

Geheime, vertrauliche und interne Informationen dürfen generell nur für Zwecke unseres Unternehmens verwendet werden. Eine darüberhinausgehende Verwendung für eigene Zwecke oder für Zwecke eines anderen Unternehmens sind strikt verboten. Das Verbot erstreckt sich auch auf die über das Auftragsverhältnis oder die Auftragsdurchführung hinausgehende Zeiten.

6 Richtiger Umgang mit Schlüssel

Die Ihnen vom Unternehmen überlassenen Schlüssel sind ausschließlich für die Verwendung durch Ihre Person bestimmt. Zutrittsmedien dürfen generell nicht an Dritte oder an Kollegen/Vorgesetzte weitergegeben werden, auch nicht temporär. Bei Fragen, Unklarheiten oder Verlust wenden Sie sich unverzüglich an die Verwaltung oder den Informationssicherheitsbeauftragten.

7 Richtiger Umgang mit schützenswerten Informationen auf Reisen

Auf den mobilen Endgeräten, die im Eigentum des externen Dienstleisters oder Lieferanten stehen oder von unserem Unternehmen zur Verfügung gestellt werden (z.B. Laptops, Handys, Smartphones, Tablets, USB-Sticks,...), sind ggf. unsere unternehmenseigene Informationen und Daten gespeichert. Verlust oder Diebstahl der können schädliche Auswirkungen für das Unternehmen haben. Daher sind die folgenden Sicherheitshinweise einzuhalten:

- Nehmen Sie grundsätzlich nur die Unterlagen, die Sie tatsächlich benötigen, mit auf Reisen.
- Bei Reisen in Drittländer (bspw. China, USA, Russland) kann nicht ausgeschlossen werden, dass Behörden bei Einreise Zugriff auf Daten von Endgeräten nehmen. Daher dürfen bei Reisen in solche Länder keine Informationen und Daten unseres Unternehmens auf den Geräten gespeichert sein.
- Speichern Sie nur die Informationen und Daten lokal und in Kopie verschlüsselt ab, die Sie tatsächlich unterwegs benötigen.
- Benachrichtigen Sie bei Verlust oder Diebstahl mobiler Endgeräte Ihren Ansprechpartner in unserem Unternehmen.
- Führen Sie keine mobilen Endgeräte ohne Passwortschutz mit sich, sofern Sie darauf Informationen und Daten unseres Unternehmens speichern.
- Geben Sie mobile Endgeräte bei Reisen nicht mit Ihrem Koffer auf.
- Lassen Sie mitgeführte Unterlagen und mobile Endgeräte nie unbeaufsichtigt (z.B. im Auto) liegen. Auch Temperaturschwankungen können nicht nur die Festplatte, sondern auch andere Speichermedien sowie das LCD-Display beschädigen.

8 Richtiges Verhalten in der Öffentlichkeit und im privaten Umfeld

Viele Geschäftsgeheimnisse werden durch Gedankenlosigkeit vor allem in Gesprächen mit Kollegen oder durch Telefongespräche in öffentlichem oder privatem Umfeld (z.B. Flugzeug, Biergarten, Restaurant) preisgegeben. Daher sind die folgenden Sicherheitshinweise einzuhalten:

- Seien Sie sich immer bewusst, worüber Sie wo kommunizieren. Achten Sie bei allen Gesprächen auf Vertraulichkeit.
- Geben Sie Informationen und Daten unseres Unternehmens in Telefongesprächen nur an persönlich bekannte Geschäftspartner preis.
- Prüfen Sie im Zweifelsfall durch einen Rückruf die Identität des Anrufers.
- Achten Sie unterwegs darauf, dass niemand einsehen kann, an welchen Informationen und Daten unseres Unternehmens Sie arbeiten (z.B. Laptop, Dokumente, etc.).
- Lassen Sie mobile Geräte nie unbeaufsichtigt.

- Geben Sie keine vertraulichen und geheimen Informationen und Daten unseres Unternehmens in privaten Gesprächen preis.
- Führen Sie keine vertraulichen Gespräche über Informationen und Daten unseres Unternehmens in der Öffentlichkeit (z.B. in Flugzeugen, in Hotels, Restaurants).
- Übermitteln Sie keine vertraulichen und geheimen Informationen über unser Unternehmen an Dritte.
- Geben Sie keine geheimen Informationen am Telefon preis.
- Geben Sie die Unternehmenshardware nicht an Familienangehörige und Dritte weiter.
- Achten Sie darauf, dass Dritte nicht die Unternehmenshardware nutzen.

9 Richtiges Verhalten im Internet und bei der E-Mail-Nutzung

Viele Geschäftsgeheimnisse werden auch durch Gedankenlosigkeit und die unsachgemäße Nutzung von elektronischen Kommunikationsmitteln preisgegeben. Daher sind die folgenden Sicherheitshinweise einzuhalten:

- Speichern Sie die Zugangsdaten zu unseren Unternehmenssystemen nicht in Ihrem Browser.
- Geben Sie keine Informationen und Daten unseres Unternehmens in sozialen Netzwerken (XING, Facebook oder ähnliche) preis, die Sie im Rahmen Ihrer Tätigkeit in unserem Unternehmen zur Kenntnis bekommen haben.
- Persönliche Profile dürfen keine Zusätze wie „arbeitet zurzeit für Kunde XXXX“ oder ähnliches enthalten.
- Besuchen Sie nur vertrauenswürdige Internetseiten.
- Klicken Sie nicht auf Links, die in SPAM-Mails oder „Kettenbriefen“ enthalten sind.
- Sofern Ihnen eine E-Mail-Account zur Verfügung gestellt wird, darf dieser ausschließt für die geschäftliche Kommunikation des Unternehmens verwendet werden. Eine private Nutzung ist ausdrücklich verboten.
- Beantworten Sie keine Emails, die persönliche Kennwörter oder PINs anfordern.
- Falls Sie am Absender der E-Mail zweifeln – nicht antworten.

10 Richtiges Verhalten in unseren Geschäftsräumen

Zur Sicherstellung der Informationssicherheit sind innerhalb unserer Geschäftsräume die folgenden Sicherheitshinweise einzuhalten:

- Externe Personen müssen am Empfang registriert werden.
- Die standortbezogenen Sicherheitshinweise müssen eingehalten werden (z.B. Fotografierverbot, Schutzausrüstung usw.).
- Fremdgeräte dürfen nicht an unsere Unternehmensnetzwerk angeschlossen werden.
- Sie erhalten ggfs. einen Zugang zu unserem Gäste-WLAN.

11 Richtiger Umgang mit Videokonferenzsystemen

Sofern möglich sollten Videokonferenzen in dafür vorgesehenen Besprechungsräumen durchgeführt werden, da hier das Risiko einer ungewollten Offenbarung von schützenswerten Informationen am geringsten ist.
Sofern aus organisatorischen Gründen Videokonferenzen nicht in dafür vorgesehenen Besprechungsräumen durchgeführt werden, sind die folgenden Sicherheitshinweise einzuhalten:

- Vor Beginn der Videokonferenz muss sichergestellt werden, dass sich keine geheimen, vertraulichen oder internen Informationen im Sichtbereich der Videokamera befinden.

- Bei Videokonferenzen sollte immer vor einer Übertragung des Videobildes sichergestellt werden, dass ein Videokonferenzhintergrund verwendet wird. Alternativ kann der Videokonferenzhintergrund auch weichgezeichnet (verschwommen) sein.
- Beim Teilen von Bildschirminhalten ist besondere Vorsicht geboten, vor allem dann, wenn Push-Benachrichtigungen und Vorschaufunktionen (z.B. bei eingehenden E-Mails etc.) aktiviert sind oder wenn verschiedene Programme auf dem PC geöffnet sind.
- Stellen Sie daher immer sicher, dass Ihre Videokonferenzpartner nur die Informationen auf Ihrem Endgerät zur Kenntnis bekommen, die tatsächlich für diesem Empfängerkreis bestimmt sind.
- Die Aufzeichnung (Speicherung) von Videokonferenzen ist nur mit vorausgehender Information und Einwilligung aller Teilnehmer zulässig.

12 Richtiger Umgang mit Speichermedien und Informationen

Auf elektronischen Speicher- und Kommunikationsmedien (z.B. Notebooks, USB-Sticks, CDs, DVDs, etc.) sind oft vertrauliche oder geheime Informationen unseres Unternehmens gespeichert. Um diese Informationen zu schützen, ist ein sicherer Umgang mit diesen Medien zwingend notwendig. Daher sind die folgenden Sicherheitshinweise einzuhalten:

- Vertrauliche Daten nur verschlüsselt auf mobilen Speichermedien speichern.
- Verstauen Sie bei Flugreisen Ihre mobilen Endgeräte im Handgepäck.
- Verwahren Sie Laptops, Handys, Schlüssel etc. sicher auf, auch außerhalb der Arbeitszeiten.
- Lassen Sie mitgeführte Unterlagen und Geräte nie sichtbar und unbeaufsichtigt (z.B. im Auto, Bahnhöfen, Flughäfen, Restaurants) liegen.
- Lassen Sie nie mobile Endgeräte unbeaufsichtigt auf Ihrem Schreibtisch liegen.
- Verwenden Sie für Informationen des Auftraggebers nur solche Cloud-Systeme, die vom Auftraggeber und dessen Informationssicherheitsbeauftragten zur Nutzung freigegeben wurden.
- Dateien in der Kategorie vertraulich/ und oder geheim werden mittels E-Mail ausgetauscht.

13 Passwörter

Zur Sicherstellung eines ausreichenden Zugangs- und Zugriffsschutzes ist es zwingend erforderlich, dass die Zugangsberechtigten mit Zugang zu den Datenverarbeitungssystemen sichere Passwörter verwenden. Jeder Zugangsberechtigte zu unseren Datenverarbeitungssystemen erhält einen ihm zugeordneten, eindeutigen Benutzernamen, mit dem der Benutzer eindeutig am jeweiligen Datenverarbeitungssystem identifiziert wird. Die nachfolgenden Passwort-Regelungen sind daher unbedingt von jedem Zugangsberechtigten einzuhalten:

- Startpasswörter, die die Zugangsberechtigten im Rahmen der ersten Anmeldung erhalten, sind umgehend durch eigene (individuelle) Passwörter zu ersetzen.
- Passwörter dürfen nicht aufgeschrieben oder am Arbeitsplatz hinterlegt werden.
- Passwörter dürfen nicht an Dritte (auch Kollegen der Abteilung) weitergegeben werden.
- Eine Anmeldung mit den Anmeldedaten eines anderen Benutzers ist verboten.
- Bei der Eingabe von Passwörtern ist darauf zu achten, dass Dritte Passwörter nicht zur Kenntnis nehmen.
- Passwörter müssen mindestens 10 Zeichen haben.
- Passwörter müssen mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten.
- Trivialpasswörter dürfen nicht verwendet werden (z.B. qwertz, 12345678, abcdefg).
- Das Geburtsdatum des Benutzers oder dessen Angehörigen darf nicht als Passwort verwendet werden.
- Passwörter müssen umgehend gewechselt werden, wenn der Verdacht besteht, dass diese kompromittiert wurden.
- Der Benutzername darf nicht Bestandteil des Passwortes sein.

- Passwörter dürfen ohne entsprechende Schutzmechanismen nicht in dem Datenverarbeitungssystem (bspw. im einem Internet-Browser) gespeichert werden.
- Die innerhalb des Unternehmens (Netzwerk) verwendeten Passwörter dürfen nicht für Anwendungen im Internet oder im privaten Umfeld verwendet werden.
- Die Speicherung der Passwörter ist nur unter Verwendung eines von unserer IT-Administration freigegebenen Passwortsafe zulässig.

14 Grundsätze beim Umgang mit personenbezogenen Daten

Beim Umgang mit personenbezogenen Daten müssen die nachfolgenden Grundsätze zwingend eingehalten werden:

- Die Verarbeitung personenbezogener Daten bedarf immer einer Rechtsgrundlage oder der nachweisbaren Einwilligung eines Betroffenen.
- Die Betroffenen müssen über die Datenverarbeitung informiert werden.
- Alle Datenverarbeitungsverfahren müssen transparent gestaltet werden.
- Personenbezogene Daten dürfen nur für den Zweck verwendet werden, für den sie tatsächlich erhoben wurden.
- Es dürfen nur die personenbezogenen Daten verarbeitet werden, die tatsächlich für die Durchführung der jeweiligen Aufgabe benötigt werden.
- Personenbezogene Daten sind immer direkt beim Betroffenen zu erheben.
- Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Bearbeitungstätigkeit notwendig ist.
- Die Möglichkeit der Anonymisierung oder Pseudonymisierung von personenbezogenen Daten ist zu berücksichtigen.
- Personenbezogene Daten müssen immer zugriffsgeschützt gespeichert bzw. verwahrt werden.
- Personenbezogene Daten müssen vor zufälligem bzw. ungewolltem Verlust geschützt werden.

15 Verhalten bei Sicherheitsvorfällen

Ein Sicherheitsvorfall liegt regelmäßig dann vor, wenn die Schutzziele der Informationssicherheit (Vertraulichkeit, Verfügbarkeit, Integrität) verletzt werden. Beispiele für einen Sicherheitsvorfall sind

- Verlust von Informationen durch Diebstahl oder unbeabsichtigte Löschung/Vernichtung.
- Verlust von Hardware durch Diebstahl oder Unachtsamkeit.
- Beschädigung von Hardware.
- Versand von Informationen per E-Mail, Telefax oder Post an einen falschen Empfänger.
- Hacking von Datenverarbeitungssystemen.
- Infizierung von Datenverarbeitungssystemen mit Schadsoftware.
- Verlust der Vertraulichkeit von Zugangsdaten zu Datenverarbeitungssystemen.
- Verlust von Schlüssel, Zutrittskarten/-token.
- Verlust von Firmen-Kreditkarten und Firmenausweis.
- Erfolglose Zugriffsversuch auf benötigte Informationen.

Sollten ein externer Dienstleister oder Lieferant feststellen oder den Verdacht haben, dass der Schutz oder die Sicherheit von Informationen oder Daten, die unserem Unternehmen zuzuordnen sind, in irgendeiner Weise gefährdet sein könnte, hat dieser sich unverzüglich an seinen Ansprechpartner zu wenden. Dies gilt insbesondere auch dann, wenn die Gefährdung sich auf personenbezogene Daten bezieht.

16 Verhalten bei einer Evakuierung

Sofern ein eingetretener Notfall eine Evakuierung unserer Geschäftsräume erfordert, müssen die nachfolgenden Regelungen zwingend eingehalten werden:

- Endgeräte müssen beim Verlassen des Arbeitsplatzes immer gesperrt werden.
- Wenn möglich sollten mobile Geräte zur Datenverarbeitung (Notebooks, Tablets, Smartphones) bei Verlassen des Gebäudes mitgenommen werden.
- Papierdokumente mit vertraulichem oder geheimem Inhalt müssen beim Verlassen des Arbeitsplatzes immer mitgenommen werden.
- Türen zu Sicherheitszonen müssen geschlossen werden. Die Türen dürfen nicht abgeschlossen werden, damit die Rettungskräfte (Feuerwehr) einen ungehinderten Zutritt zu den Räumen haben.
- Der offiziell ausgewiesene Sammelplatz ist unverzüglich aufzusuchen.
- Den Anweisungen der Notfallbeauftragten und der Rettungskräfte ist Folge zu leisten.

17 Beendigung des Projekts

Spätestens bei Beendigung des Projektes sind sämtliche Daten an unser Unternehmen zurückzugeben und den korrekten Erhalt der Daten bestätigen zu lassen.
Elektronisch gespeicherte Informationen sind so zu löschen, dass die Informationen nachträglich nicht wiederhergestellt werden können. Die vollständige Löschung muss gegenüber unserem Unternehmen in Textform bestätigt werden.

18 Kontaktdaten

Unseren Informationssicherheitsbeauftragten erreichen Sie wie folgt:

Marco Eisenried

0841/96809-26

m.eisenried@l-a-t.de

Unsere IT-Administration erreichen Sie wie folgt:

Marco Eisenried

0841/96809-26

m.eisenried@l-a-t.de

19 Aktualisierung/Überwachung

Der Informationssicherheitsbeauftragte und die Geschäftsleitung stellen die Aktualität dieser Informationssicherheitsrichtlinie sicher. Dazu wird im Rahmen der regelmäßig stattfindenden Regelkommunikation der Änderungsbedarf ermittelt und dokumentiert. Die relevanten externen Dienstleister und Lieferanten werden über die vorgenommenen Änderungen informiert.