Informationssicherheit für Auftragnehmer

Richtlinie

Frank Eppinger/GF

Öffentlich

Inhaltsverzeichnis

1 Einführung und Zweck

Die GTÜ mbH ist eine jeweils durch die DAkkS nach DIN EN ISO/IEC 17020 (Inspektionsstellen) beziehungsweise ISO/IEC 17025 (Prüf- und Kalibrierlabore) zertifizierte Organisation, deren Geschäftszweck die Bereitstellung von Prüf-, Inspektions- und Zertifizierungsdienstleistungen im Automobil- und Verkehrssicherheitssektor ist.

Informationssicherheit spielt eine zentrale Rolle in der Erfüllung der Aufgaben der GTÜ mbH und deren Tochtergesellschaften GTÜ Anlagensicherheit GmbH, GTÜ Certification GmbH und GTÜ Prüfmittelservice GmbH (kurz GTÜ), da die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowohl für das Vertrauen als auch die Qualität der angebotenen Dienstleistungen für Behörden, Kunden und Partner gleichermaßen wichtig ist.

Die GTÜ betreibt ein Informationssicherheitsmanagementsystem (ISMS) gemäß TISAX® und ISO 27001:2022. Zur Aufrechterhaltung der Normanforderungen sowie gesetzlicher und regulatorischer Vorgaben ist die GTÜ verpflichtet, die Informationssicherheit bei Auftragnehmern*) (kurz AN) sicherzustellen.

Die GTÜ ist sich der Bedeutung des Schutzes von Informationen bewusst, da deren Missbrauch zu großen materiellen und immateriellen Schäden führen kann. Aus diesem Grund sind AN verpflichtet, die vorliegende Richtlinie einzuhalten.

2 Geltungsbereich

Diese Richtlinie gilt für AN der GTÜ.

3 Informationssicherheit und Schutzziele

Alle Informationen, die AN im Rahmen der Geschäftsanbahnung und vertraglichen Leistungserbringung zugänglich sind, überlassen oder hergestellt werden, werden als wirtschaftliche Werte betrachtet. Informationen können in unterschiedlicher Form vorliegen – z.B. in elektronischer Form als Datei, in physischer Form als Ausdruck oder als gesprochenes Wort.

Der Wert der Informationen bemisst sich an der Wichtigkeit und Kritikalität bezogen auf die Wertschöpfung und fließt in Risikobetrachtungen hinsichtlich materieller und immaterieller Schäden (z. B. Kapital- oder Reputationsverlust) ein.

Alle Informationen sind vom AN hinsichtlich der folgenden Schutzziele zu schützen

- **Vertraulichkeit:** Sicherstellung, dass nur autorisierte Personen Zugang zu sensiblen und vertraulichen Informationen haben, und

- **Integrität:** Gewährleistung der Genauigkeit und Vollständigkeit der Informationen und Verhinderung unautorisierter Änderungen, und

- **Verfügbarkeit:** Sicherstellung, dass Informationen und Dienstleistungen stets für befugte Personen zugänglich sind, wenn sie benötigt werden.

Jeder AN ist ein wichtiger und aktiver Bestandteil der Informationssicherheit der GTÜ. Als solcher hat er Informationssicherheit unter Berücksichtigung der o. g. Aspekte jederzeit geeignet umzusetzen.

4 Klassifizierte Informationen

Die GTÜ definiert vier Arten von Informationen, die geschützt werden müssen. Der AN verpflichtet sich mit Informationen entsprechend ihrer Klassifizierung wie folgt umzugehen:

Vertrauliche und streng vertrauliche Informationen – Informationen, bei deren Verletzung der Schutzziele die Erreichung von Unternehmenszielen (streng vertraulich) oder das Erreichen von Produkt- und Projektzielen (vertraulich) gefährdet werden kann. Zu dieser Kategorie gehören Prototypen-Informationen sowie personenbezogene Daten. Die Weitergabe der Informationen an Dritte ist untersagt. Die Weitergabe der Informationen ist nur an Mitarbeiter des AN gestattet, die an der Leistungserbringung beteiligt sind und die Information unmittelbar zur Erfüllung einer konkreten Aufgabe im Rahmen der Leistungserbringung benötigen („Need-To-Know"-Prinzip).

Interne Informationen – Informationen, die ausschließlich für Mitarbeiter der GTÜ und autorisierte Auftragnehmer bestimmt sind, bei deren Verletzung der Schutzziele die Erreichung von Unternehmenszielen oder das Erreichen von Produkt- und Projektzielen jedoch nicht gefährdet wird. Die Weitergabe der Informationen an Dritte oder nicht an der Leistungserbringung beteiligter Mitarbeiter des AN ist untersagt.

Öffentliche Informationen – Informationen, die offengelegt werden dürfen. Informationen dürfen vom AN nur offengelegt werden, wenn:

- Die Information als öffentlich klassifiziert ist, oder

- Die GTÜ die Information zur Weitergabe freigegeben hat, oder

- Dies zum Zweck der vertraglich vereinbarten Leistung zwingend erforderlich ist.

Bei unbekannter Klassifizierung ist stets von „vertraulich" auszugehen.

5 Allgemeine Regelungen und Verantwortung

5.1 Allgemeine Sicherheitsmaßnahmen

Bei Unterbeauftragungen durch den AN hat der AN sicherzustellen, dass dem Unterauftragnehmer (UAN) die Inhalte dieser Richtlinie bekannt gemacht sind.

AN und ggf. UAN setzen nur qualifiziertes Personal ein und unterweisen ihre Mitarbeiter eigenverantwortlich zu relevanten gesetzlichen, regulatorischen und vertraglichen Anforderungen und Richtlinien.

AN und UAN sollten ein ISMS nach anerkanntem Standard betreiben. Dies ist nachzuweisen durch

- Entweder eine Zertifizierung (bei Auftragsverarbeitung personenbezogener Daten oder Verarbeitung personenbezogener Daten besonderer Kategorie sowie Informationen der Klassifizierung „vertraulich" oder „streng vertraulich")

- Oder eine Selbstauskunft (bei der Verarbeitung von Informationen der Klassifizierung „intern" bzw. „öffentlich" sowie in begründeten und von der GTÜ genehmigten Ausnahmen)

Der Nachweis eines ausreichenden Sicherheitsniveaus des AN kann über ein Audit durch die GTÜ oder einen durch die GTÜ beauftragten und geeigneten Dienstleister überprüft werden.

Darüber hinaus verpflichtet sich der AN dazu:

- Informationen nur zum Zweck, der Dauer und dem notwendigen Umfang der Leistungserbringung zu verarbeiten, und

- Sorgfältig mit den Informationswerten der GTÜ umzugehen, diese insbesondere gegen unberechtigten Zugang oder Zugriff zu schützen und eine Verletzung der Vertraulichkeit, Integrität und Verfügbarkeit zu vermeiden oder zu verhindern, und

- Gesetzliche, regulatorische und vertragliche Bestimmungen, insbesondere die DSGVO, das BDSG-neu, Lizenz- und Urheberrechte sowie Handels- und Steuergesetze einzuhalten und gegebenenfalls den vorgeschriebenen Meldepflichten zu entsprechen, und

- Die Rechte und Interessen der GTÜ und ihrer Mitarbeiter zu schützen.

5.2 Grundlagen der zulässigen Nutzung der GTÜ-Ressourcen

Alle durch die GTÜ bereitgestellten Ressourcen wie Hardware, Software, digitale Dienste, Ver- und Entsorgungseinrichtungen sowie sonstige Anlagen

und Systeme der GTÜ werden ausschließlich zum Zweck der vertraglichen Leistungserbringung zur Verfügung gestellt. Bei der Nutzung der von der GTÜ bereitgestellten Ressourcen verpflichtet sich der AN Folgendes zu beachten:

+ Jede Nutzung hat – soweit möglich - ressourcenschonend und werterhaltend zu erfolgen, und

+ Jede Nutzung erfolgt nur mit entsprechender Legitimation und zum festgelegten Zweck, und

+ Unsachgemäße Nutzung, Missbrauch oder (auch teilweise) Beschädigung sind als Informationssicherheitsvorfall gem. Kapitel 6 zu melden, und

+ Eine Nutzung findet in Eigenverantwortung nach den Prinzipien „Need-To-Know" statt. Selbst wenn technisch oder organisatorisch die Möglichkeit einer weitergehenden Nutzung besteht, beschränkt sich der AN auf die Aktionen, die im Rahmen der Erfüllung des aktuellen Arbeitsauftrags erforderlich sind.

5.3 Technische und organisatorische Regelungen

Bei der Leistungserbringung für die GTÜ verpflichtet sich der AN die folgenden technischen und organisatorischen Regelungen einzuhalten:

Hardware – Von der GTÜ bereitgestellte Hardware ist im überlassenen Zustand unverändert zu verwenden und nach Gebrauch umgehend zurückzugeben. Insbesondere sind keine Schutzmaßnahmen zu umgehen, zu ändern oder auszuschalten (z. B. Anti-Schadsoftware abschalten, gesperrte Ports). Verlust, Fehlfunktion oder Beschädigung haben ohne Verzögerung als Informationssicherheitsvorfall gem. Kapitel 6 gemeldet zu werden.
Vom AN eingebrachte Hardware darf ausschließlich der Leistungserbringung dienen. Sie hat dem Stand der Technik zu entsprechen und alle allgemeinen Sicherheitsanforderungen und rechtlichen Vorgaben zu erfüllen.

Mobilgeräte und mobile Datenträger – Mobilgeräte und mobile Datenträger müssen die allgemeinen Anforderungen an Hardware erfüllen. Die Verschlüsselung von Informationen muss gewährleistet sein. Es ist jederzeit für sichere Aufbewahrung und Transport zu sorgen.

Netzwerk – In Netzwerken der GTÜ dürfen nur Geräte der GTÜ oder von der GTÜ genehmigte Geräte betrieben werden. Bei GTÜ-fremden Netzwerken ist auf starke Verschlüsselung nach Stand der Technik und zuverlässige Anbieter zu achten. Im Zweifel ist Internetzugang über das eigene Mobiltelefon herzustellen.

Benutzer-Accounts und Authentifizierung – PINs und Passwörter sind nach Stand der Technik auszuwählen (Länge und Komplexität) und sicher aufzubewahren. Für unterschiedliche Accounts sind verschiedene Passwörter einzusetzen. Initialkennwörter sind nach der ersten Anmeldung zu ändern.

Wenn möglich ist Multi-Faktor-Authentifizierung (MFA) zu verwenden. Anmeldeinformationen sind unter keinen Umständen zu teilen.

Software – Zur Leistungserbringung darf seitens des AN nur lizensierte Software aus sicheren Quellen verwendet werden. Die Software muss auf dem aktuellen Versions- und Patch-Stand sein. Aus der Nutzung der Software dürfen keine ungewollten Verpflichtungen wie etwa Rechte Dritter entstehen. Von der GTÜ bereitgestellte Software darf nur zur Leistungserbringung im Rahmen des bestehenden Auftrags verwendet und nur im Rahmen vorgeschriebener Aktualisierungen verändert werden.

Hosting außerhalb der EU, Nutzung von Cloud-Diensten, SaaS und Künstliche Intelligenz – Hosting außerhalb der EU, Nutzung von Cloud-Diensten, SaaS und Künstlicher Intelligenz bedürfen der vorherigen schriftlichen Genehmigung der GTÜ.

E-Mail – Bei der Verwendung von E-Mail sind die allgemeinen Sicherheitsvorgaben zu beachten (Achtung vor Phishing!). Von der GTÜ bereitgestellte E-Mail-Konten sind nur zur Auftragserfüllung bzw. zu geschäftlichen Zwecken zu verwenden. Die Verwendung privater E-Mail-Accounts ist untersagt.
Für die Übermittlung von Dateien sollte eine sichere Austauschplattform verwendet werden, die auf Anfrage durch die GTÜ bereitgestellt wird. In begründeten Ausnahmen ist auch die Übermittlung per E-Mail mit verschlüsselten Anhängen erlaubt. Passwörter sind getrennt zu übermitteln. Bei mindestens als vertraulich eingestuften Kommunikationsinhalten sind E-Mails vollständig zu verschlüsseln.
Es muss sichere E-Mail-Infrastruktur verwendet werden, Mail-Server müssen dem Stand der Technik entsprechen, einen aktuellen Softwarestand haben und sicher konfiguriert sein.

Informationsübertragung – Eine Übertragung von Informationen findet ausschließlich über von der GTÜ vorgegebenen sicheren Lösungen statt. Als (streng) vertraulich klassifizierte Informationen müssen verschlüsselt sein. Ausnahmen müssen schriftlich vereinbart sein. Bei Ausnahmen ist auf verschlüsselte Übertragung und Speicherung sowie eine protokollierte Zugriffssteuerung zu achten. Bei Telefonaten ist auf eine vertrauliche Umgebung zu achten.

Informationsverarbeitung – Informationen der GTÜ oder Informationen, die im Auftrag der GTÜ erstellt oder verarbeitet werden, müssen getrennt von Informationen Dritter verarbeitet und gespeichert werden. Ein unberechtigter Zugriff durch Dritte muss angemessen unterbunden sein (z. B. durch Rechtemanagement).

Remote-Zugriff und Mobiles Arbeiten – Arbeitsorte außerhalb der Liegenschaften der GTÜ müssen bekannt gemacht und vertraglich vereinbart sein. Bei Arbeiten von außerhalb der Liegenschaften der GTÜ muss eine sichere Arbeitsumgebung gewährleistet sein. Für Fernzugriffe sind ausschließlich von der GTÜ bereitgestellte oder genehmigte Lösungen zu verwenden. Arbeiten

außerhalb der Europäischen Union bedarf der schriftlichen Zustimmung der GTÜ.

Unterbeauftragung und Personalwechsel – Eine Unterbeauftragung muss vor Vertragsbeginn oder zum frühestmöglichen Zeitpunkt – in jedem Fall aber vor der Unterbeauftragung - in Schriftform angezeigt werden. Jede Unterbeauftragung bedarf der schriftlichen Zustimmung der GTÜ.
Veränderungen beim Schlüsselpersonal des AN für die Leistungserbringung muss ebenfalls vor Vertragsbeginn oder zum frühestmöglichen Zeitpunkt in Schriftform angezeigt werden. Ein Personalwechsel darf nur erfolgen, wenn nachweislich eine vergleichbare Qualifikation gewährleistet ist und die ordnungsgemäße Leistungserbringung in keiner Weise beeinträchtigt wird.

Aufzeichnungen, Bild und Ton – Jede Art von Aufzeichnung hat ausnahmslos im Rahmen der vertraglichen Leistungserbringung zu erfolgen und ist entweder durch festgelegte Verfahren implizit oder durch die GTÜ explizit genehmigt. Die Verwendung von Bild- und Ton-Aufzeichnungsgeräten bedarf der schriftlichen Vereinbarung.

Einbehalten, Weitergabe und Rückgabe von Informationen – Eine Weitergabe an Dritte ist nur zur Erfüllung des Auftragszwecks oder entsprechender Rechtsgrundlage erlaubt und bedarf der schriftlichen Zustimmung durch die GTÜ. Nach Vertragsbeendigung oder nach Aufforderung sind alle Informationen an die GTÜ zurückzugeben oder nach vorheriger Zustimmung der GTÜ zu vernichten, jeweils unter Berücksichtigung vertraglicher oder gesetzlicher Vorgaben (z. B. Beendigungsunterstützung, Backups, gesetzliche Aufbewahrungs- bzw. Löschpflichten). Auf Anforderung der GTÜ hat der AN einen Nachweis für die Vernichtung der Informationen zu erbringen. Darüber hinaus ist das Einbehalten von Informationen verboten.

Datenschutz und Umgang mit personenbezogenen Daten – Für den Umgang mit personenbezogenen Daten wird höchstmögliche Vertraulichkeit vorausgesetzt. Eine Verarbeitung von Daten im Auftrag der GTÜ als Verantwortlicher im Sinne des Datenschutzes bedarf des zusätzlichen Abschlusses eines Vertrags zur Auftragsverarbeitung.

6 Auskunft zur Informationssicherheit und Meldung von Vorfällen

Auskünfte zur Informationssicherheit und Fragen zu dieser Richtlinie beantwortet der Informationssicherheitsbeauftragte der GTÜ unter informationssicherheit@gtue.de.

Informationssicherheitsvorfälle – also die Gefährdung oder Verletzung von Schutzzielen – mit möglichen, auch verzögerten Auswirkungen auf die GTÜ oder die vertraglichen Leistungen sind unmittelbar an den fachlichen Ansprechpartner der GTÜ sowie an informationssicherheit@gtue.de oder über +49 (0) 711 976 76 444 zu melden. Dies gilt insbesondere bei der Zerstörung, unerlaubten Veränderung, dem Diebstahl oder der (angedrohten) illegitimen

Offenlegung von nicht als öffentlich klassifizierten Informationen sowie bei Verdacht oder Vorliegen eines behördlich meldepflichtigen oder kriminellen Sachverhalts.

7 Gültigkeit und Überprüfung der Einhaltung der Richtlinie

Die Verpflichtung zur Einhaltung dieser Richtlinie ist Bedingung für die Auftragsannahme und tritt spätestens mit Vertragsabschluss in der zu diesem Zeitpunkt gültigen Version in Kraft.

Die GTÜ hat das Recht, im Benehmen mit dem AN Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Die GTÜ hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Richtlinie durch den AN in dessen Geschäftsbetrieb während der üblichen Geschäftszeiten zu überzeugen.

*) Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Technik braucht Sicherheit.

GTÜ Gesellschaft für
Technische Überwachung mbH
Vor dem Lauch 25
70567 Stuttgart

FON 0711 97676-0
MAIL info@gtue.de
WEB www.gtue.de