



Nachhaltigkeit bei Klüh: strukturiert und transparent!

Informationssicherheit

Unternehmerische Verantwortung, wertorientiertes Handeln und gleichbleibend hohe Qualität unserer Dienstleistungen – das ist uns wichtig. Deshalb setzt Klüh entlang der gesamten Wertschöpfungskette hohe Standards, die über gesetzliche Anforderungen hinausgehen – insbesondere in den Bereichen **soziale, ökologische und ökonomische Nachhaltigkeit**.

In der Reihe „Nachhaltigkeit bei Klüh: strukturiert und transparent!“ informieren wir themenbezogen über den aktuellen Stand unseres Nachhaltigkeitspfades.

Informationssicherheit und Nachhaltigkeit hängen eng zusammen, da beide darauf abzielen, Risiken zu minimieren und langfristige Stabilität zu sichern.

Eine sichere IT-Infrastruktur schützt sensible Daten vor Cyberangriffen und unterstützt eine ressourcenschonende und effiziente Nutzung von IT-Systemen. Ein wirksames Informationssicherheitsmanagement verhindert Datenverluste, stärkt das Vertrauen von Kunden und Partnern und trägt damit zu einer verantwortungsvollen, nachhaltigen Unternehmensführung bei.



Informationssicherheit

Informationssicherheit – der rechtliche Rahmen

In Deutschland gelten nationale und europäische Gesetze sowie Vorschriften, die maßgeblich zur Informationssicherheit im geschäftlichen Bereich beitragen. Neben datenschutzrechtlichen Anforderungen (siehe Flyer „Datenschutz im Unternehmen“) prägen insbesondere europäische Regelwerke den regulatorischen Rahmen der Cyber- und IT-Sicherheit.

Hierzu zählen unter anderem die **NIS-2-Richtlinie** zur Stärkung der Cybersicherheit wichtiger Einrichtungen, der **AI Act** zur Regulierung von Systemen der künstlichen Intelligenz, der **Cyber Resilience Act (CRA)** mit Sicherheitsanforderungen für Produkte mit digitalen Elementen sowie die **CER-Richtlinie** (Critical Entities Resilience Directive) zum Schutz kritischer Infrastrukturen.

Für einzelne Branchen gelten darüber hinaus zusätzliche Vorgaben. So verpflichtet der **Digital Operational Resilience Act (DORA)** Unternehmen im Finanzsektor zu umfassenden Maßnahmen zur Sicherstellung ihrer digitalen Resilienz. Auch im Bereich der **Luftsicherheit** bestehen besondere Anforderungen. Die Identifikation kritischer informations- und kommunikationstechnischer Systeme und Daten (KIKS) erfolgt unter anderem auf Grundlage der **EU-Verordnung 2015/1998**, die Sicherheitsanforderungen für den Luftverkehr festlegt.

In Deutschland kommt dem **Bundesamt für Sicherheit in der Informationstechnik (BSI)** eine zentrale Rolle zu. Mit dem IT-Grundschutz stellt das BSI einen etablierten Standard für Informationssicherheitsmanagement bereit. Darüber hinaus verpflichtet das **IT-Sicherheitsgesetz (IT-SiG)** Betreiber kritischer Infrastrukturen, angemessene Schutzmaßnahmen umzusetzen und Sicherheitsvorfälle zu melden.

Zertifizierungen

Neben gesetzlichen Vorgaben gibt es auch Zertifizierungs- und Prüfstandards, mit denen Unternehmen ihr Engagement für Informationssicherheit über gesetzliche Mindestanforderungen hinaus nachweisen können. Viele Kunden fordern heute entsprechende Standards zunehmend als Voraussetzung für eine Zusammenarbeit.

In der Automobilindustrie hat sich beispielsweise **TISAX** (Trusted Information Security Assessment Exchange) etabliert. Dieser Standard ermöglicht es Unternehmen, den Schutz vertraulicher Informationen – etwa von Prototypen oder Entwicklungsdaten – nach einheitlichen Anforderungen prüfen zu lassen.

Eine branchenübergreifend anwendbare und international etablierte Norm ist die **ISO/IEC 27001:2022**. Sie gilt als führender Standard zur Implementierung eines **Informationssicherheits-Managementsystems (ISMS)**.

Im Rahmen der Norm werden Informationen systematisch bewertet und nach ihrem Schutzbedarf klassifiziert.

Auf Basis einer strukturierten Risikoanalyse werden Ziele, Maßnahmen und Kontrollen definiert, um Informationen im gesamten Unternehmen zu schützen – von der physischen Zugangskontrolle über IT-Systeme bis hin zur Zusammenarbeit mit Lieferanten und Kunden.

Wesentliche Bestandteile sind zudem ein umfassendes **Risikomanagement** sowie regelmäßige **Schulungen der Mitarbeitenden**, um ein nachhaltiges Sicherheitsbewusstsein im Unternehmen zu fördern.

Umsetzung bei Klüh

Klüh erfüllt branchenspezifische Anforderungen, beispielsweise im Bereich der **Luftsicherheit** (KIKS). Bei Bedarf können auch zusätzliche branchenspezifische Prüfstandards wie **TISAX** umgesetzt werden.

Der Fokus liegt derzeit auf der Implementierung und Ausweitung der **ISO/IEC-27001-Zertifizierung**. Seit 2025 ist die AES/NSL des Geschäftsbereiches Security nach ISO/IEC 27001:2022 zertifiziert. Ein schrittweiser Rollout auf weitere Unternehmensbereiche ist bis 2027 geplant.

Vorteile der Zertifizierung nach ISO 27001

- Effektiver Schutz von Informationen, Daten und Geschäftsprozessen
- Systematische Umsetzung von Risikomanagement und regulatorischen Anforderungen
- Förderung des Sicherheitsbewusstseins der Mitarbeitenden
- Kostenreduzierung durch die Vermeidung von Sicherheitsvorfällen

Durch die Zertifizierung stellt Klüh sicher, dass hohe Standards der Informationssicherheit eingehalten werden und schafft damit eine vertrauensvolle Grundlage für die Zusammenarbeit mit Kunden und Partnern.

Die Resilienz von Informationssystemen, der Schutz sensibler Daten sowie ein wirksames Risikomanagement leisten darüber hinaus einen wichtigen Beitrag zu nachhaltigen und stabilen Geschäftsmodellen.

Haben Sie Fragen oder wünschen Sie weitere Informationen? Nachfolgende Ansprechpersonen helfen Ihnen gerne weiter:

Informationssicherheitsbeauftragter

Stefan von der Lahr, s.vonderlahr@klueh.de

Leiter Qualitätsmanagement | Nachhaltigkeit

Rainer Schultes, r.schultes@klueh.de

Geschäftsführer Security

Sven Horstmann, s.horstmann@klueh.de

