



SICHERHEITSRICHTLINIE INFORMATIONEN

von Eurodies Italia S.r.l.

Vom Vorstand genehmigt am 28.11.2025



Inhaltsverzeichnis

1. Einleitung	3
2. Zweck des Dokuments	3
3. Umfang	4
4. Rollen und Verantwortlichkeiten im Bereich Informationssicherheit	4
5. Grundsätze für den verantwortungsvollen Umgang mit Informationen	5
6. Ziele für die Informationssicherheit von Eurodies Italia S.r.l.	6
7. Berichte	7
8. Aktualisierung, Verbreitung und Kommunikation	8



1. Vorwort

Eurodies Italia S.r.l. (im Folgenden „Eurodies“, „Unternehmen“ oder „Unternehmen“) ist sich bewusst, dass es in einem Kontext arbeitet, der durch hohe Anforderungen an **Vertraulichkeit, Zuverlässigkeit, Schutz des technischen Know-hows** und **den Schutz von** Informationen, die mit Kunden, Partnern und anderen Interessengruppen der Automobillieferkette geteilt werden, gekennzeichnet ist.

In diesem Dokument definiert das Unternehmen die Prinzipien, Richtlinien und Verpflichtungen, die eingegangen sind, um eine angemessene Verwaltung der Informationssicherheit sicherzustellen, wobei die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Daten und Informationen gewährleistet sind, unabhängig vom Format, Medium oder System, durch das sie erzeugt, empfangen, gespeichert, übertragen oder verarbeitet werden.

In diesem Zusammenhang verpflichtet sich Eurodies dazu, **Produkte und Dienstleistungen anzubieten, die den** von den Kunden gestellten Anforderungen und den spezifischen Bedürfnissen des Automobilsektors entsprechen, und verfolgt einen **strukturierten Ansatz** im Informationssicherheitsmanagement, der den besten Referenzpraktiken und den Anforderungen des **TISAX-Programms** entspricht (Vertrauenswürdiger Informationssicherheitsbewertungsaustausch). Die Einhaltung des TISAX-Zertifizierungsprozesses ist ein wesentliches Instrument für das Unternehmen, um sein Governance-System zu stärken, die Zuverlässigkeit seiner Prozesse zu demonstrieren und transparent auf Kundenerwartungen in Bezug auf den Informationsschutz zu reagieren.

Eurodies erkennt an, dass im Automobilsektor das sichere Management von Informationen einen strategischen Wert erhält, insbesondere im Hinblick auf den Schutz technischer Daten, Zeichnungen, Entwurfsspezifikationen, kommerziellen Informationen, Prototypen, vertraulicher Dokumente und aller anderen Elemente der Unternehmensinformationsressourcen oder von Dritten empfangenen Elemente. Der Schutz dieser Informationen ist eine grundlegende Voraussetzung für die Wahrung der Geschäftskontinuität, des Unternehmensrufs, des Kundenvertrauens und der Wettbewerbsfähigkeit des Unternehmens.

Eurodies ist sich voll bewusst, dass Bedrohungen für die Informationssicherheit ein wachsendes **Risiko darstellen**, auch aufgrund der fortschreitenden Digitalisierung, der Vernetzung von Produktions- und Designprozessen sowie der zunehmenden Komplexität der Beziehungen entlang der Automobillieferkette. Aus diesem Grund verpflichtet sich das Unternehmen, geeignete organisatorische, technische und verfahrenstechnische Maßnahmen zu ergreifen, um unbefugten Zugriff, Verlust, Änderungen, Nichtverfügbarkeit oder unzulässige Offenlegung von Informationen zu verhindern.

2. Zweck des Dokuments

Die Informationssicherheitspolitik zielt darauf ab, die von Eurodies Italia Italia S.r.l. eingegangenen Prinzipien und Verpflichtungen zu definieren, um den Schutz der im Rahmen ihrer be-



trieblichen, designbezogenen, Produktions- und kommerziellen Aktivitäten verwalteten Informationen zu gewährleisten, mit besonderem Fokus auf die Bedürfnisse des Automobilsektors.

Mit diesem Dokument beabsichtigt Eurodies, **die Informationsressourcen des Unternehmens** sowie die von Kunden, Partnern, Lieferanten und anderen Interessenten erhaltenen Informationen zu schützen und dessen Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.

Eurodies erkennt Informationssicherheit als ein wesentliches Element an, um die Geschäftskontinuität, das Vertrauen der Kunden, die Einhaltung der geltenden Anforderungen und die Wettbewerbsfähigkeit des Unternehmens sicherzustellen. Die Richtlinie leitet zudem **das Verhalten und die Verantwortlichkeiten der an** den Unternehmensprozessen beteiligten Personen und fördert Risikobewusstsein, Unfallprävention und kontinuierliche Verbesserung im Einklang mit dem TESAX-Bewertungs- und Zertifizierungsprozess.

3. Umfang

Die in diesem Dokument enthaltene Richtlinie gilt **für alle von Eurodies Italia S.r.l. verwalteten Informationen**, unabhängig vom Format, Medium oder Verarbeitungsmethode, einschließlich elektronischer, papierbasierter, mündlicher oder sonstiger verfügbarer Form im Rahmen der Unternehmensaktivitäten.

Das Anwendungsgebiet umfasst IT-Systeme, Netzwerkinfrastrukturen, Anwendungen, Geräte, physische und digitale Archive sowie Personalwesen, die an Geschäftsprozessen beteiligt sind, mit besonderem Bezug auf betriebliche, Design-, Produktions-, kommerzielle und administrative Tätigkeiten.

Die Richtlinie ist für alle Mitarbeiter, Mitarbeitende, Lieferanten, Partner und Dritte bindend, die aus irgendeinem Grund Unternehmensdaten, Dokumente und Informationen verarbeiten, nutzen oder darauf Zugriff haben oder von Kunden und anderen Interessenten erhalten haben. Angemessene Sicherheitsmaßnahmen sind in jeder Phase des Informationslebenszyklus erforderlich, einschließlich der Erstellung, des Empfangs, der Klassifizierung, Nutzung, Speicherung, Übertragung, Weitergabe, Lagerung und, wo zutreffend, des Löschens oder Löschens von Informationen.

4. Rollen und Verantwortlichkeiten im Bereich Informationssicherheit

Die Gesamtverantwortung für die Informationssicherheit liegt beim **Vorstand**, der die strategischen Leitlinien festlegt, den Text der Richtlinie genehmigt, eine Unternehmenskultur fördert, die auf den Schutz von Informationswerten ausgerichtet ist, und die Verfügbarkeit der für die Umsetzung angemessener organisatorischer, technischer und verfahrensrechtlicher Maßnahmen notwendiger Ressourcen sicherstellt.

Sie fördert außerdem Informations-, Schulungs- und Sensibilisierungsinitiativen für Personal



und andere Beteiligte, damit jeder sich der Risiken im Zusammenhang mit der Informationsverwaltung sowie der korrekten Nutzung von IT-Tools, Unternehmenssystemen und der verarbeiteten Dokumentation bewusst ist, insbesondere im Bereich technischer, gestaltungsbezogener und vertraulicher Informationen im Automobilsektor.

Der **vom Management ernannte IT-Manager** hat die Aufgabe, das ordnungsgemäße Funktionieren der IT-Infrastruktur des Unternehmens sicherzustellen, die Implementierung von Sicherheitsmaßnahmen zu unterstützen, das Management von Zugriffen und Autorisierungen zu überwachen, die Zulässigkeit der Systeme zu überwachen und zur Identifizierung etwaiger Schwachstellen oder Verbesserungsbedarf beizutragen. Zu seinen Aufgaben gehören außerdem die Überwachung von IT-Dienstleistern, die Überprüfung der Einhaltung vertraglicher Vereinbarungen sowie die Überwachung der Nutzung autorisierter und regelmäßig lizenzierter Software.

Alle Unternehmensfunktionen, die an der Verwaltung von Daten, Dokumenten, Informationssystemen und digitalen Werkzeugen beteiligt sind, müssen gemäß den geltenden Gesetzen, dem *Organisation-, Management- und Kontrollmodell*, internen Verfahren und Unternehmensbestimmungen zur Verarbeitung, dem Schutz und dem Management von Informationen arbeiten. Die Aktivitäten müssen nach **den Prinzipien der Korrektheit, Transparenz, Genauigkeit, Vollständigkeit und Trennung der Aufgaben** durchgeführt werden, ebenso wie durch eine korrekte Zuweisung und regelmäßige Überprüfung der Zugangsprofile.

Alle Mitarbeiter, Mitarbeiter und Dritte, die auf Unternehmensinformationen oder -systeme zugreifen, sind im Umfang ihrer Kompetenz für die Einhaltung der vom Unternehmen festgelegten Regeln verantwortlich. Insbesondere sind sie verpflichtet, IT-Tools ausschließlich für Arbeitszwecke zu nutzen, ihre Zugangsdaten sorgfältig zu schützen, diese nicht an Dritte weiterzugeben, keine unautorisierte Software zu installieren, keine Sicherheitsmaßnahmen zu umgehen und sich nicht an Verhaltensweisen zu beteiligen, die die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen gefährden könnten.

Jede beteiligte Partei ist außerdem verpflichtet, **alle Anomalien**, Vorfälle, unbefugten Zugriffe, Schwachstellen, nicht konformes Verhalten oder Situationen, die der Informationssicherheit schaden könnten, umgehend zu melden und dabei aktiv zur Verhinderung von IT-Risiken, zum Schutz des Unternehmenswissens und zur kontinuierlichen Verbesserung des Informationssicherheitsmanagementsystems beizutragen.

5. Prinzipien für verantwortungsvolle Informationsverarbeitung

Eurodies verfolgt einen systemischen Ansatz im Informationssicherheitsmanagement, der auf folgenden Grundprinzipien basiert:

- **Vertraulichkeit**
Der Zugang zu Informationen darf nur berechtigten Personen gewährt werden, abhängig von der innehabten Rolle, den durchgeführten Aktivitäten und den tatsächlichen operativen Bedürfnissen.



- **Integrity**
Information muss vollständig, genau, aktuell und vor unbefugten Änderungen, Änderungen oder Löschungen geschützt sein, um ihre Zuverlässigkeit über die Zeit zu gewährleisten.
- **Verfügbarkeit**
Unternehmensinformationen, Systeme und Werkzeuge müssen zeitweise und auf die Weise zugänglich sein, die für die Durchführung von Aktivitäten und die Geschäftskontinuität erforderlich ist.
- **Eurodies**
verpflichtet sich, die geltenden Gesetze, Vorschriften, vertraglichen Anforderungen und Standards einzuhalten, einschließlich solcher in Bezug auf den Schutz personenbezogener Daten, Informationssicherheit sowie den TESAX-Bewertungs- und Zertifizierungspfad.
- **Risikomanagement**
Informationssicherheitsrisiken werden durch einen strukturierten Ansatz identifiziert, bewertet und behandelt, der darauf abzielt, mögliche negative Auswirkungen auf Geschäftsabläufe, Kunden und andere Interessengruppen zu verhindern oder zu verringern.
- **Verantwortlichkeiten**
Alle an der Verwaltung, Nutzung oder dem Zugang zu Informationen beteiligten Parteien sind für den ordnungsgemäßen Schutz der Informationen im Einklang mit ihrer Rolle, ihren Aktivitäten und den geltenden Geschäftsabläufen verantwortlich.
- **Kontinuierliche**
VerbesserungDas Informationssicherheitsmanagementsystem wird im Laufe der Zeit überwacht, bewertet und aktualisiert, um seine Wirksamkeit zu verbessern, bestehende Schutzmaßnahmen zu stärken und auf die Entwicklung von Risiken, Technologien und anwendbaren Anforderungen zu reagieren.

6. Ziele für die Informationssicherheit von Eurodies Italia S.r.l.

Eurodies verpflichtet sich, den Schutz von Unternehmensinformationen und vertraulichen Informationen, die von Kunden, Partnern, Lieferanten und anderen Interessengruppen empfangen werden, durch die Anwendung organisatorischer, technischer und verfahrensrechtlicher Maßnahmen zu gewährleisten, die dem jeweiligen Kontext entsprechen und mit den geltenden Anforderungen, einschließlich derjenigen, die im TESAX-Bewertungs- und Zertifizierungsprozess vorgesehen sind.

Zu diesem Zweck definiert Eurodies folgende Ziele für ein effektives Informationssicherheitsmanagement:



- Ein **Informationssicherheitsmanagementsystem übernehmen, warten und im Laufe der Zeit verbessern**, das für die Aktivitäten des Unternehmens und die damit verbundenen Risiken angemessen ist;
- Risiken im Zusammenhang mit Informationssicherheit **zu identifizieren und regelmäßig zu bewerten**, geeignete Präventions-, Minderungs- und Kontrollmaßnahmen zu definieren und umzusetzen;
- **Formalisieren und anwenden von Verfahren und Betriebsanweisungen** für Zugriffsmanagement, physischen und logischen Schutz von Informationen, Sicherheit von IT-Systemen, Backup-Management und Geschäftskontinuität;
- **Mitarbeiterbewusstsein und Schulungen fördern**, um eine Sicherheitskultur zu fördern und sicherzustellen, dass jede Person sich der Risiken und Schutzmaßnahmen bewusst ist, die für ihre Rolle gelten;
- **Relevante Lieferanten und Subunternehmer bewerten und überwachen**, damit ein angemessener Schutz der geteilten Informationen gewährleistet ist;
- **Unfälle, unbefugten Zugriff, Verlust, Änderungen, Nichtverfügbarkeit oder unsachgemäße Weitergabe von Informationen** zu verhindern;
- **Überwachen** Sie die Wirksamkeit der ergriffenen Maßnahmen und aktualisieren Sie die Ziele regelmäßig entsprechend der Entwicklung von Risiken, Technologien, regulatorischen Anforderungen und Kundenerwartungen.

Um sein Engagement messbar zu machen, definiert Eurodies auch diese quantitativen Ziele:

- Sicherstellen, dass bis 2027 mindestens 90 % der Mitarbeitenden **regelmäßige Schulungen zur Informationssicherheit erhalten**;
- Stellen Sie sicher, dass 100 % der Unternehmensnutzer **persönliche Zugangsdaten und Systemautorisierungen haben, die streng auf die ausgeführten Aufgaben beschränkt** sind.

7. Empfehlungen

Eurodies fördert ein Geschäftsumfeld, das auf **Integrität, Verantwortung und Transparenz** basiert und fördert die rechtzeitige Meldung von rechtswidrigem Verhalten, Verstößen gegen das *Organisations-, Management- und Kontrollmodell gemäß dem Gesetzesdekret 231/2001* sowie Nichteinhaltung von Unternehmensverfahren oder Verhaltensweisen, die die Informationssicherheit gefährden könnten.

Das Unternehmen hat den Empfängern einen internen **Kanal** zur Meldung erheblicher rechtswidriger Handlungen gemäß Gesetzesdekret 231/2001 zur Verfügung gestellt; Verstöße gegen das Modell oder andere Situationen, die dem Unternehmen potenziell schaden, einschließlich aller Verstöße oder kritischer Fragen im Zusammenhang mit Verwaltung, Schutz und Sicherheit von Informationen.



Dieser Kanal arbeitet in Übereinstimmung mit D.LGS. Nr. 24/2023 zu *Whistleblowing*.

Meldungen können auch anonym auf folgende Weise gemacht werden:

- In **schriftlicher Form über die Whistleblowing-Plattform**, die über den eigenen Link auf der Unternehmenswebsite und unter der Adresse erreichbar ist <https://eurodies.integrity.complylog.com/>.
- In **mündlicher Form** durch Registrierung, gemäß den vom Unternehmensverfahren vorgegebenen Verfahren.

Berichte werden gemäß den im Absatz „Berichte“ beschriebenen Verfahren und im Absatz „Maßnahmen in Anwendung der in D erwähnten Disziplin“ übermittelt und verwaltet. LGS. 24/2023“ des allgemeinen Teils des Modells selbst und insbesondere auf der Grundlage des „Verfahrens zur Verwaltung von Berichten gemäß D.LGS. 24/2023“ vom Unternehmen übernommen.

Eurodies garantiert die **Vertraulichkeit der Identität des Whistleblowers**, der beteiligten Personen und des Inhalts des Berichts in Übereinstimmung mit den geltenden Vorschriften. Der **Schutz des Whistleblowers vor jeglicher Form von Vergeltung**, Diskriminierung oder Bestrafung im Zusammenhang mit der in gutem Glauben erstellten Meldung wird ebenfalls gewährleistet, ohne die Möglichkeit zu beeinträchtigen, anonyme Meldungen gemäß den vom Unternehmensverfahren vorgesehenen Verfahren zu machen.

8. Aktualisierung, Verbreitung und Kommunikation

Der Vorstand von Eurodies sorgt dafür, dass die Informationssicherheitsrichtlinie an alle Mitarbeiter, Mitarbeiter und, wo zutreffend, an Dritte weitergegeben wird, die an der Verwaltung oder dem Zugang zu Unternehmensinformationen beteiligt sind, auf eine Weise, die deren Wissen und effektive Anwendung gewährleistet.

Die Richtlinie wird **mindestens jährlich überprüft** und in jedem Fall immer dann, wenn Aktualisierungen aufgrund regulatorischer Änderungen, der Entwicklung geltender Anforderungen, Aktualisierungen der Best Practices, Anforderungen im Zusammenhang mit dem TISAX-Bewertungs- und Zertifizierungsprozess oder bedeutender organisatorischer, technologischer und operativer Änderungen erforderlich sind.

Alle Aktualisierungen dieses Dokuments werden vom Vorsitzenden genehmigt und **den relevanten Empfängern umgehend** über die als am passendsten erachteten Kanäle mitgeteilt, darunter:

- E-Mails an Mitarbeiter;
- Veröffentlichung oder Veröffentlichung am schwarzen Brett des Unternehmens;
- Zustellung oder Teilen bei der Einstellung neuer Mitarbeiter;



- Teilen beim Abschluss oder Verlängern von Verträgen mit Lieferanten, Partnern oder anderen relevanten Dritten.

Eurodies setzt sich außerdem dafür ein, das Verständnis der Inhalte der Richtlinie durch angemessene Kommunikation, Informations- und Sensibilisierungsinitiativen zu fördern, sodass alle Beteiligten über die Prinzipien, Verpflichtungen und Verantwortlichkeiten im Zusammenhang mit Informationssicherheit informiert sind.

Avigliana (TO), 28.11.2025

- **Die Leitung**