POLITICA PER LA SICUREZZA DELLE INFORMAZIONI di Eurodies Italia S.r.l.

Approvato dal Consiglio di Amministrazione in data 28.11.2025

Indice

1. Premessa

Eurodies Italia S.r.l. (di seguito "Eurodies", "Società" o "Azienda") è consapevole di operare in un contesto caratterizzato da elevati requisiti di **riservatezza, affidabilità, protezione del know-how tecnico** e **tutela delle informazioni** condivise con clienti, partner e altri stakeholder della filiera automotive.

La presente Politica ha lo scopo di definire i principi, gli indirizzi e gli impegni assunti da Eurodies per garantire un'adeguata gestione della sicurezza delle informazioni, assicurando la riservatezza, l'integrità e la disponibilità dei dati e delle informazioni trattate, indipendentemente dal formato, dal supporto o dal sistema attraverso cui esse sono generate, ricevute, conservate, trasmesse o elaborate.

In tale prospettiva, Eurodies si impegna a **erogare prodotti e servizi conformi ai requisiti** stabiliti dai clienti e alle esigenze specifiche del settore automotive, adottando un **approccio strutturato** alla gestione della sicurezza delle informazioni coerente con le migliori pratiche di riferimento e con i requisiti previsti dallo schema **TISAX** (Trusted Information Security Assessment Exchange). L'adesione al percorso di certificazione TISAX rappresenta per l'Azienda uno strumento essenziale per rafforzare il proprio sistema di governance, dimostrare l'affidabilità dei propri processi e rispondere in modo trasparente alle aspettative dei clienti in materia di protezione delle informazioni.

Eurodies riconosce infatti che, nel settore automobilistico, la gestione sicura delle informazioni assume un valore strategico, con particolare riferimento alla protezione di dati tecnici, disegni, specifiche progettuali, informazioni commerciali, prototipi, documentazione riservata e ogni altro elemento del patrimonio informativo aziendale o ricevuto da terze parti. La tutela di tali informazioni costituisce un presupposto fondamentale per preservare la continuità operativa, la reputazione aziendale, la fiducia dei clienti e la competitività dell'Impresa.

Eurodies è pienamente consapevole che le minacce alla sicurezza delle informazioni rappresentano un **rischio** crescente, anche in ragione della progressiva digitalizzazione, dell'interconnessione dei processi produttivi e progettuali e della crescente complessità delle relazioni lungo la catena di fornitura automotive. Per questo motivo, l'Azienda si impegna ad adottare misure organizzative, tecniche e procedurali adeguate a prevenire accessi non autorizzati, perdita, alterazione, indisponibilità o divulgazione indebita delle informazioni.

2. Scopo del documento

La presente Politica ha lo scopo di definire i principi e gli impegni assunti da Eurodies Italia S.r.l. per garantire la protezione delle informazioni gestite nell'ambito delle proprie attività operative, progettuali, produttive e commerciali, con particolare riferimento alle esigenze del settore automotive.

Attraverso la presente Politica, Eurodies intende **tutelare il patrimonio informativo aziendale** e le informazioni ricevute da clienti, partner, fornitori e altre parti interessate, assicurandone riservatezza, integrità e disponibilità.

Eurodies riconosce la sicurezza delle informazioni come elemento essenziale per garantire la continuità operativa, la fiducia dei clienti, la conformità ai requisiti applicabili e la competitività dell'Azienda. La Politica orienta inoltre **comportamenti e responsabilità delle persone coinvolte** nei processi aziendali, promuovendo consapevolezza dei rischi, prevenzione degli incidenti e miglioramento continuo, in coerenza con il percorso di valutazione e certificazione TISAX.

3. Campo di applicazione

La presente Politica si applica **a tutte le informazioni gestite da Eurodies Italia S.r.l.,** indipendentemente dal formato, dal supporto o dalle modalità di trattamento, incluse le informazioni in formato elettronico, cartaceo, verbale o comunque disponibili nell'ambito delle attività aziendali.

Il campo di applicazione comprende i sistemi informatici, le infrastrutture di rete, gli applicativi, i dispositivi, gli archivi fisici e digitali, nonché le risorse umane coinvolte nei processi aziendali, con particolare riferimento alle attività operative, progettuali, produttive, commerciali e amministrative.

La Politica è vincolante per tutti i dipendenti, collaboratori, fornitori, partner e soggetti terzi che, a qualsiasi titolo, trattano, utilizzano o accedono a dati, documenti e informazioni aziendali o ricevute da clienti e altre parti interessate. L'adozione di adeguate misure di sicurezza è richiesta in ogni fase del ciclo di vita delle informazioni, incluse la creazione, ricezione, classificazione, utilizzo, archiviazione, trasmissione, condivisione, conservazione e, ove applicabile, eliminazione o distruzione delle stesse.

4. Ruoli e responsabilità per la sicurezza delle informazioni

La responsabilità complessiva in materia di sicurezza delle informazioni è affidata al Consiglio di Amministrazione, che definisce gli indirizzi strategici, approva la presente Politica, promuove una cultura aziendale orientata alla protezione del patrimonio informativo e assicura la disponibilità delle risorse necessarie per l'attuazione di adeguate misure organizzative, tecniche e procedurali. Esso promuove inoltre iniziative di informazione, formazione e sensibilizzazione rivolte al personale e alle altre figure coinvolte, affinché ciascuno sia consapevole dei rischi connessi alla gestione delle informazioni e delle corrette modalità di utilizzo degli strumenti informatici, dei sistemi aziendali e della documentazione trattata, con particolare riferimento alle informazioni tecniche, progettuali e riservate del settore automotive.

Il **Responsabile IT**, nominato dalla Direzione, ha il compito di garantire il corretto funzionamento dell'infrastruttura informatica aziendale, supportare l'implementazione delle misure di sicurezza, presidiare la gestione degli accessi e delle abilitazioni, monitorare l'adeguatezza dei sistemi e contribuire all'identificazione di eventuali vulnerabilità o esigenze di miglioramento. Rientrano inoltre tra le sue responsabilità il monitoraggio dei fornitori di servizi IT, la verifica del rispetto degli accordi contrattuali e il controllo sull'utilizzo di software autorizzati e regolarmente licenziati.

Tutte le funzioni aziendali coinvolte nella gestione di dati, documenti, sistemi informativi e strumenti digitali sono tenute a operare nel rispetto della normativa applicabile, del Modello di organizzazione, gestione e controllo, delle procedure interne e delle disposizioni aziendali in materia di trattamento, protezione e gestione delle informazioni. Le attività devono essere svolte secondo **principi di correttezza, trasparenza, accuratezza, completezza e segregazione dei compiti**, anche attraverso una corretta attribuzione e verifica periodica dei profili di accesso.

Tutti i dipendenti, collaboratori e soggetti terzi che accedono alle informazioni o ai sistemi aziendali sono responsabili, per quanto di competenza, del rispetto delle regole definite dall'Azienda. In particolare, sono tenuti a utilizzare gli strumenti informatici esclusivamente per finalità lavorative, custodire con diligenza le proprie credenziali, non divulgarle a terzi, non installare software non autorizzati, non aggirare i presidi di sicurezza e non porre in essere condotte che possano compromettere la riservatezza, l'integrità o la disponibilità delle informazioni.

Ciascun soggetto coinvolto è inoltre tenuto a **segnalare tempestivamente eventuali anomalie**, incidenti, accessi non autorizzati, vulnerabilità, comportamenti non conformi o situazioni potenzialmente pregiudizievoli per la sicurezza delle informazioni, contribuendo attivamente alla prevenzione dei rischi informatici, alla tutela del know-how aziendale e al miglioramento continuo del sistema di gestione della sicurezza delle informazioni.

5. Principi per la gestione responsabile delle informazioni

Eurodies adotta un approccio sistemico alla gestione della sicurezza delle informazioni, fondato sui seguenti principi chiave:

- **Riservatezza**
  L'accesso alle informazioni deve essere consentito esclusivamente ai soggetti autorizzati, in funzione del ruolo ricoperto, delle attività svolte e delle effettive necessità operative.
- **Integrità**
  Le informazioni devono essere complete, accurate, aggiornate e protette da modifiche, alterazioni o cancellazioni non autorizzate, al fine di garantirne l'affidabilità nel tempo.
- **Disponibilità**
  Le informazioni, i sistemi e gli strumenti aziendali devono essere accessibili nei tempi e secondo le modalità necessarie allo svolgimento delle attività e alla continuità operativa.
- **Conformità**
  Eurodies si impegna a rispettare le leggi, le normative, i requisiti contrattuali e gli standard applicabili, inclusi quelli relativi alla protezione dei dati personali, alla sicurezza delle informazioni e al percorso di valutazione e certificazione TISAX.
- **Gestione del rischio**
  I rischi connessi alla sicurezza delle informazioni sono identificati, valutati e trattati attraverso un approccio strutturato, volto a prevenire o ridurre possibili impatti negativi sulle attività aziendali, sui clienti e sulle altre parti interessate.

- **Responsabilità**
  Tutti i soggetti coinvolti nella gestione, utilizzo o accesso alle informazioni sono responsabili della loro corretta protezione, in funzione del proprio ruolo, delle attività svolte e delle procedure aziendali applicabili.
- **Miglioramento continuo**
  Il sistema di gestione della sicurezza delle informazioni è monitorato, valutato e aggiornato nel tempo, al fine di migliorarne l'efficacia, rafforzare i presidi esistenti e rispondere all'evoluzione dei rischi, delle tecnologie e dei requisiti applicabili.

6. Obiettivi per la sicurezza delle informazioni di Eurodies Italia S.r.l.

Eurodies si impegna a garantire la tutela delle informazioni aziendali e delle informazioni riservate ricevute da clienti, partner, fornitori e altre parti interessate, attraverso l'adozione di misure organizzative, tecniche e procedurali adeguate al contesto in cui opera e coerenti con i requisiti applicabili, inclusi quelli previsti dal percorso di valutazione e certificazione TISAX.

A tal fine, Eurodies definisce i seguenti obiettivi per una gestione efficace della sicurezza delle informazioni:

- adottare, mantenere e migliorare nel tempo un **Sistema di Gestione della Sicurezza delle Informazioni** adeguato alle attività aziendali e ai rischi connessi;
- identificare e valutare periodicamente i **rischi relativi alla sicurezza delle informazioni**, definendo e attuando idonee misure di prevenzione, mitigazione e controllo;
- **formalizzare e applicare procedure e istruzioni operative** per la gestione degli accessi, la protezione fisica e logica delle informazioni, la sicurezza dei sistemi informatici, la gestione dei backup e la continuità operativa;
- **promuovere la consapevolezza e la formazione del personale**, al fine di diffondere una cultura della sicurezza e garantire che ciascuna risorsa conosca i rischi e le misure di protezione applicabili al proprio ruolo;
- **valutare e monitorare** i fornitori e i subappaltatori rilevanti, affinché sia garantito un adeguato livello di protezione delle informazioni condivise;
- **prevenire** incidenti, accessi non autorizzati, perdita, alterazione, indisponibilità o divulgazione indebita delle informazioni;
- monitorare l'efficacia delle misure adottate e aggiornare periodicamente gli obiettivi in funzione dell'evoluzione dei rischi, delle tecnologie, dei requisiti normativi e delle aspettative dei clienti.

Al fine di rendere misurabile il proprio impegno, Eurodies definisce inoltre i seguenti obiettivi quantitativi:

7. garantire che almeno il 90% del personale riceva entro il 2027 **formazione periodica in materia di sicurezza delle informazioni**;
8. assicurare che il 100% degli utenti aziendali disponga di **credenziali di accesso individuali** e sia sottoposto a **profilazione degli accessi** coerente con il proprio ruolo e con le attività svolte.

9. Segnalazioni

Eurodies promuove un ambiente aziendale fondato su **integrità, responsabilità e trasparenza**, incoraggiando la segnalazione tempestiva di eventuali condotte illecite, violazioni del Modello di organizzazione, gestione e controllo ex D.Lgs. 231/2001, non conformità alle procedure aziendali o comportamenti che possano compromettere la sicurezza delle informazioni.

La Società si è dotata di un **canale interno** attraverso cui i Destinatari possono segnalare condotte illecite rilevanti ai sensi del D.Lgs.231/2001 o violazioni del Modello, oltre ad altre situazioni potenzialmente pregiudizievoli per l'Azienda, incluse eventuali violazioni o criticità connesse alla gestione, protezione e sicurezza delle informazioni.

Tale canale opera nel rispetto del D.Lgs. n. 24/2023 in materia di *Whistleblowing*.

Le segnalazioni possono essere effettuate, anche in forma anonima, secondo le seguenti modalità:

- In **forma scritta tramite piattaforma WhistleBlowing** dedicata: raggiungibile attraverso il link presente sul sito web aziendale e al seguente indirizzo: https://eurodies.integrity.complylog.com/.
- In forma orale, tramite registrazione, secondo le modalità previste dalla procedura aziendale.

Tali segnalazioni sono trasmesse e vengono gestite secondo le modalità descritte nel paragrafo "Segnalazioni" e nel paragrafo "Misure in applicazione della disciplina di cui al D.Lgs. 24/2023" della parte generale del Modello stesso e, in particolare, sulla base della "Procedura di gestione delle segnalazioni ai sensi del D.Lgs.24/2023" adottata a tal fine dalla Società.

Eurodies garantisce la **riservatezza dell'identità del segnalante**, delle persone coinvolte e del contenuto della segnalazione, nel rispetto della normativa applicabile. È inoltre assicurata la **tutela del segnalante da qualsiasi forma di ritorsione**, discriminazione o penalizzazione connessa alla segnalazione effettuata in buona fede, ferma restando la possibilità di effettuare segnalazioni anonime secondo le modalità previste dalla procedura aziendale.

10. Aggiornamento, diffusione e comunicazione

Il Consiglio di Amministrazione di Eurodies assicura la diffusione della presente Politica a tutti i dipendenti, collaboratori e, ove applicabile, ai soggetti terzi coinvolti nella gestione o nell'accesso

a informazioni aziendali, secondo modalità idonee a garantirne la conoscenza e l'effettiva applicazione.

La Politica è oggetto di **revisione almeno annuale** e, in ogni caso, ogniqualvolta si rendano necessari aggiornamenti in ragione di modifiche normative, evoluzione dei requisiti applicabili, aggiornamenti delle migliori pratiche di riferimento, esigenze connesse al percorso di valutazione e certificazione TISAX o cambiamenti organizzativi, tecnologici e operativi rilevanti.

Eventuali aggiornamenti della presente Politica sono approvati dal Presidente e **comunicati tempestivamente ai destinatari** interessati attraverso i canali ritenuti più opportuni, tra cui:

- invio tramite e-mail ai dipendenti;
- affissione o pubblicazione nella bacheca aziendale;
- consegna o condivisione in fase di assunzione di nuovo personale;
- condivisione in fase di stipula o rinnovo di contratti con fornitori, partner o altri soggetti terzi rilevanti.

Eurodies si impegna inoltre a promuovere la comprensione dei contenuti della Politica attraverso adeguate iniziative di comunicazione, informazione e sensibilizzazione, affinché tutte le persone coinvolte siano consapevoli dei principi, degli impegni e delle responsabilità connessi alla sicurezza delle informazioni.

Avigliana (TO), 28.11.2025

La Direzione