Job Description | *Security Compliance Manager*

We are seeking a passionate Security Compliance Manager to join our growing team.

1.   ABOUT ELTEMATE

We are ELTEMATE – A Hogan Lovells Legal Tech Company. Our goal is to make clients' lives easier by delivering practical solutions to everyday problems. We combine a deep understanding of our customers' legal needs with the speed and innovation of a technology start-up. Our portfolio covers a large spectrum of legal tech solutions including artificial intelligence, eDiscovery, information analysis, regulatory updates, databases, deal rooms, workflow management, case management, document automation, risk assessment, reporting, and apps.

With our headquarters in Amsterdam and offices in Germany, the UK, Singapore, Brazil and the US, we are a truly global team of around 100 professionals. Our diverse and international workforce thrives on collaboration, creativity, and expertise.

If you're ready to make an impact in legal tech and work in an inspiring global setting, we'd like to hear from you.

2.   ROLE DESCRIPTION

As our Security Compliance Manager, you will play a critical role in maintaining and improving our information security management system and ensuring that our products and operations meet the highest standards of (cyber)security, privacy, AI and regulatory compliance. You will help lead our efforts to obtain and maintain key certifications (including ISO 27001, ISO 27701, and ENX TISAX), help comply with cybersecurity regulations such as NIS2 and DORA. You will work closely with teams across product, engineering, infrastructure, legal, privacy and management to define and monitor secure product development practices, implement compliance policies, and ensure that security controls meet both internal standards and external regulatory requirements. Risk management will also be part of your responsibilities, including maintaining the risk register, assessing IT and product-related risks, and developing risk treatment plans that include mitigation measures for potential risks and remediation activities for identified gaps. You will also serve as a point of contact for external auditors,

regulators, and customers during security due diligence processes, assessments, and certifications.

3. DUTIES AND RESPONSIBILITIES

- Support the planning, documentation, implementation, and maintenance of our ISMS, with a strong focus on achieving and maintaining certifications such as ISO 27001, ENX TISAX, and ISO 27701.
- Manage and update a risk register, including the identification, assessment, and tracking of IT, security and other compliance risks.
- Review, document and approve security requirements and controls integrated into product development, including access management, encryption, and other (cyber)security, privacy and data protection measures.
- Collaborate with the engineering team to define, document and implement secure software development practices and monitor adherence throughout the product lifecycle.
- Conduct and oversee vendor assessments and risk assessments; act as the primary point of contact for vendor security and compliance reviews and audits.
- In collaboration with the engineering and privacy teams draft, implement, document and communicate security and cybersecurity compliance policies, standards, and procedures in alignment with regulatory requirements.
- Deliver security awareness and compliance training across the organization.
- Stay informed about evolving cyber threats, security standards, and regulatory requirements.

4. REQUIRED KNOWLEDGE, SKILLS AND EXPERIENCE

- At least 5-7 years of experience in security compliance, risk management, or cybersecurity.
- Proven track record with frameworks like ISO 27001, ISO 27701, ENX TISAX, US NIST Framework, or with SOC 2 compliance.
- Solid knowledge of IT governance, risk management, and compliance frameworks.
- Proven experience in conducting vendor assessments, including security questionnaires, risk management, and developing risk treatment plans with defined remediation activities.
- Strong understanding of ISMS, risk management, and technical security controls.
- Familiarity with emerging regulatory frameworks such as DORA, NIS2, CRA, and the EU AI Act, and the requirements therein.
- Strong documentation and policy drafting skills, and ability to communicate and coordinate with stakeholders effectively.
- Fluent in English, both written and spoken.

5. OTHER PREFERRED SKILLS

- Background in regulated industries (e.g., legal, automotive, finance).
- Familiarity with emerging regulatory frameworks such as DORA, NIS2, CRA, and the EU AI Act.
- Well versed with GDPR and other data protection laws.

- Experience with using GRC platforms (e.g., OneTrust, COMPYL and ServiceNow).
- Experience in implementing security governance requirements in Microsoft Azure would be an advantage.
- Comfortable delivering (cyber)security awareness and compliance training.

6. OTHER DETAILS

- Full-time preferred, but negotiable for the right candidate.
- Start date: Preferably immediately.
- Location: Preferably in Amsterdam (the Netherlands), but other locations are also possible (EU, such as Germany) as we can accommodate agile work environments.
- Hybrid work model.
- Background screening is part of the hiring process.
- Compensation depending on qualifications and experience.

7. DISCLAIMER

ELTEMATE is an equal employment opportunity employer and does not discriminate against any employee or applicant for employment on the basis of race, color, religion, gender identity, national origin, age, disability, veteran status, marital status, sexual orientation, or any other characteristic protected by law.

If you are interested, please get in touch with us by sending your resume and motivation at hr@eltemate.com. We look forward to meeting you. Please note: We manage our recruitment in-house and do not work with agencies.