aginion

Incident Response Statement

Aginion Luxembourg

Date: 2026-07-20

Classification: Public

Purpose

This statement describes how Aginion Luxembourg ("we") prepares for, detects, and responds to security incidents affecting our services or the data our customers entrust to us, and how and when we communicate with affected customers. It is provided for the information of our customers and prospective customers. It summarises our approach; it is not our internal incident-response procedure, and it is not a contractual warranty. Binding notification terms are set out in the applicable service agreement and Data Processing Agreement.

What we treat as an incident

We treat as a security incident any event that compromises, or is reasonably likely to compromise, the confidentiality, integrity, or availability of our services or of customer data. This includes a personal data breach — a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data we process on a customer's behalf.

Our approach

We maintain a documented incident-response process, owned by the Chief Information Security Officer (CISO) and exercised on a regular basis. Our response follows established phases:

- Detection and analysis — we operate monitoring and detection controls across our systems, and we assess reports received from our staff, our customers, and our vulnerability-disclosure channel to confirm and classify incidents.
- Containment — we act to limit the scope and impact of a confirmed incident.
- Eradication and recovery — we remove the cause and restore affected services, drawing on our business-continuity and disaster-recovery arrangements.
- Post-incident review — after significant incidents we conduct a review to identify root cause and improve our controls.

We classify incidents by severity so that our response and communication are proportionate to their impact.

Notification and communication

Our role is that of an ICT service provider and, for personal data, a processor. Where an incident affects a customer's data or services, we notify that customer so that they — as controller, or as the regulated entity — can meet their own obligations, with our support.

- Affected customers. We notify affected customers without undue delay after confirming an incident that affects their data or services, and in any event within 24 hours of confirmation. We provide updates as our understanding develops.
- Personal data breaches. Where we become aware of a personal data breach affecting data we process for a customer, we notify that customer without undue delay, with the information they need to assess the breach and to meet their own duties — including any duty to notify their supervisory authority within 72 hours.
- Support for regulatory reporting. For customers subject to sector obligations — for example NIS2 or DORA — our notifications are designed to provide the information and timing they need to make their own reports to competent authorities, including at the successive reporting stages those regimes require.

- What a notification contains. As far as known at the time, we describe the nature of the incident, the systems and data affected, the likely consequences, and the measures taken or proposed. We update the notification as further information becomes available.

We do not make regulatory notifications on a customer's behalf unless separately agreed; the customer, as controller or regulated entity, remains responsible for its own reporting, and we support it.

Cooperation

We cooperate with affected customers throughout an incident, including with their own investigations and, where appropriate, with competent authorities and forensic specialists, as provided in the applicable agreements.

Testing and improvement

Our incident-response process is reviewed and exercised regularly, and is updated in light of exercises, real incidents, and changes to our services and threat environment.

Related documents

This statement should be read alongside our business-continuity and disaster-recovery statement, our vulnerability-disclosure policy, our ISO/IEC 27001 certification, and — for the relevant customers — our GDPR, DORA, and NIS2 statements.

Governance and review

This statement is reviewed at least annually, and sooner if triggered by a material change in our process, our services, or the applicable law.

- End of Document -

aginion

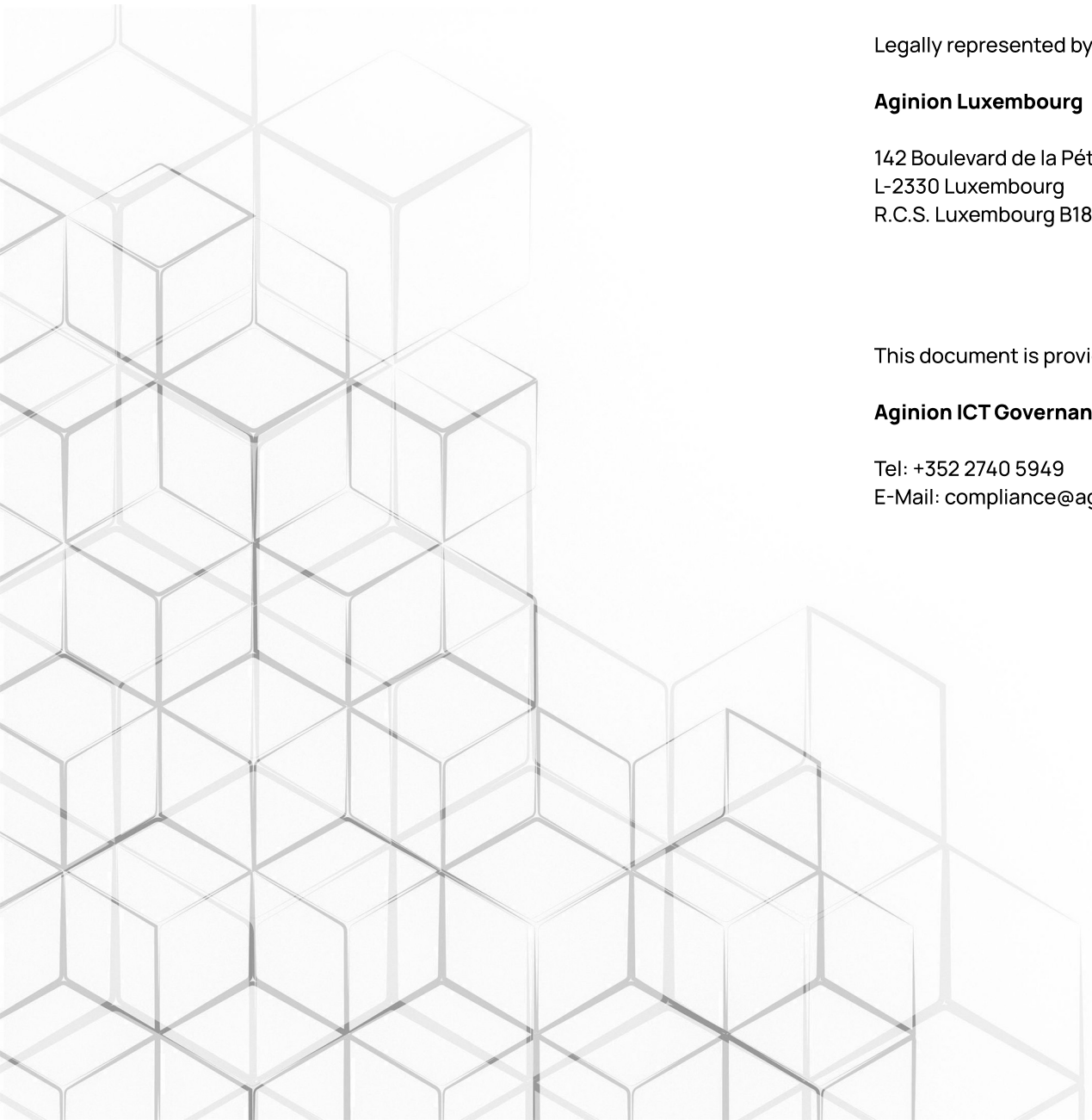
Aginion Group

Legally represented by:

Aginion Luxembourg

142 Boulevard de la Pétrusse
L-2330 Luxembourg
R.C.S. Luxembourg B184509

This document is provided by:

Aginion ICT Governance

Tel: +352 2740 5949
E-Mail: compliance@aginion.com