



Voluntary Sustainability Report

2025

Content

Message from the Chief Executive Officer	1	7 Social and societal information	29
1 Business model	2	7.1 Company Workforce	29
2 Sustainability strategy 2024–2030	5	7.2 Governance of social issues	32
2.1 Cybersecurity as an enabler of sustainability	5	7.3 Social Dialogue and Engagement	33
2.3 Strategic pillars	5	7.4 Ensuring fair and attractive remuneration and benefits	36
2.2 Strategy development process	6	7.5 Career and Skills Development	37
2.4 Initiative CyberESG	6	7.6 Human and Labour Rights commitments	42
3.4 Membership requirements for the CyberESG community	7	7.7 Diversity, Equity and Inclusion (DE&I)	43
3 Sustainability governance framework	9	7.8 Health and Safety	46
3.1 Mission	9	7.9 Consumers and end-users	48
3.2 Governance Structure	9	8 Corporate culture and business conduct policies	54
3.2.1 Governance Structure and Oversight	11	8.1 Compliance governance and organisation	54
4 Analysis of material Impacts, Risks and Opportunities (IROs)	12	8.2 Ethics, prevention and the fight against corruption	55
4.1 Process for analysing double materiality	12	8.3 Transparency and the fight against tax evasion	60
4.2 Key ESG-related risks and opportunities identified	16	8.4 Export Controls	61
5 Exclusive Networks' sustainability commitments	17	9 Methodological note	63
5.5 Roadmap to address sustainability issues	18	9.1 Scope of consolidation	63
6 Environmental Information	19	9.2 Preparation and compilation of this voluntary non financial disclosure	63
6.1 Governance of environmental questions	19	9.4 GRI correspondance table and alignment with SDGs	65
6.2 Climate Change	20	9.5 SASB correspondance table	68
6.2 Methodological note	23	10 Opinion of the independent notified body	69
6.2.1 Scope of consolidation	23	APPENDIX 1	72
6.2.1 Carbon footprint methodology	25		

Message from the Chief Executive Officer

Dear Reader,

2025 has been a year that tested convictions, and strengthened them.

The completion of our acquisition by Clayton, Dubilier & Rice and Permira marks a new chapter for Exclusive Networks. It raises the bar on accountability and reinforces our ambition to build a stronger business, capable of creating lasting value for all its stakeholders.

The world we operate in is becoming more connected, more interdependent and more fragile. As the World Economic Forum noted in 2026, cyber resilience is becoming a defining condition for economic stability, operational continuity and trust. Artificial intelligence is reshaping the threat landscape, accelerating both attack and defense, while geopolitical, regulatory and environmental pressures are adding new layers of complexity for organizations everywhere.

In this context, the responsibility of a company like ours extends beyond the products we distribute. Our sustainability strategy for 2024–2030 is built on a simple conviction: a secure digital world is an essential enabler of a sustainable one.

Our position in the cybersecurity ecosystem gives us both reach and responsibility. As a global cybersecurity specialist, we can contribute not only through the way we operate, but also through the standards we promote across our partnerships, the expertise we bring to the value chain, and the skills and awareness we help build across the broader ecosystem.

Progress has been real and yet we remain clear-eyed about what lies ahead. We have foundations to strengthen, targets to refine, cultural shifts to deepen, and the outcomes of our double materiality assessment to translate into concrete action. What we know with certainty is that meaningful progress requires awareness, education, collaboration and discipline.

Our people are the engine of this transformation. In 2025, we continued to build a more unified global company across more than 50 countries, we invested in the culture, tools and programs that help make sustainability not a standalone function, but part of how we think, act and engage with our partners, vendors and customers.

Sustainability is not a destination. It is the discipline of making better decisions, every day, at every level of the organization. We are proud of the ground we have covered, and clear about how far we still have to go.

Jesper Trolle,

**Chief Executive Officer
Exclusive Networks**

1 Business model

A Global Cybersecurity

Sector TRENDS

A \$50 bn accessible market growing by 92% in 4 years

High needs for cybersecurity: a strategic risk, rising number of attacks

Increasingly complex range of products and solutions

RESOURCES

Highly skilled workforce

- **3102** employees across **50+** countries
- **22 %** engineers
- **42 %** sales representatives
- **41 %** women / **52 %** men
- **1,200+** cyber and cloud certified technical and sales people

Cybersecurity & IT ecosystem

Unique knowledge of cybersecurity and IT ecosystem

- **+ 320** global vendors reach local customers
- **Exclusive Training Centres (ETCs)** delivering worldwide technical education and accreditation
- **Cyber Lab**
- Training the next generation in cybersecurity (**CyberFarm**)
- Rich **talent acquisition & pipeline** (IT veterans)

Global Partners Network

Worldwide scale, local implementation

- **40+** warehouses
- **4** main logistic centres
- Trusted relationships with more than **20,000 reseller partners**
- (Local) resellers reach a global customer base
- (Local) vendors reach a global customer base
- Proprietary channel data (20 years of sales data)

Financial capital

- **Strong balance sheet**

Global & digital operations

- **Sales Operations team**
- **Exclusive Access:** customer platforms for digital demos and order management
- **Data Forge, oSpace and Elastic digital** (demand & lead generation in development)
- **4 ASC** (authorized support centres)
- **Global supply chain** for multi-country deals & **4 hubs** for supply



VISION

A fully reliable digital world, made more secure by the most innovative technologies.

UNIQUE POSITIONING in a complex ecosystem

DIVERSIFIED VENDORS, emerging, established



EXCLUSIVE NETWORKS

RESELLER PARTNERS: consulting, systems integrators, managed services providers

THOUSANDS OF ORGANIZATIONS to protect

5 STRATEGIC PILLARS



Take advantage of the underlying growth of our vendors and the wider Cybersecurity market in current geographical regions



Extend the geographical coverage of our partnerships with our existing vendors

specialist



MISSION

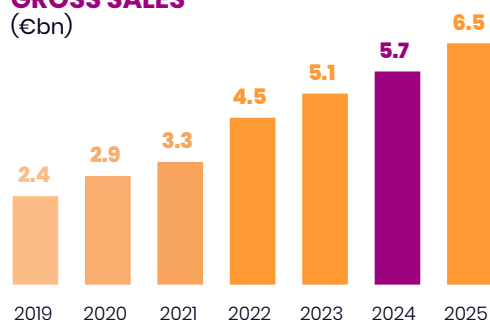
To be the leading trusted global cybersecurity go-to-market specialist.

SUSTAINABLE GROWTH

More than 20 ACQUISITIONS in 10 years
INCLUDING DAN Distribution in 2025

Strong track record of profitable growth

GROSS SALES (€bn)



Enter into new partnerships with cybersecurity solutions providers to complement the solutions offered in our portfolio



Develop our services range to strengthen our value offering and boost customer loyalty



Pursue our external growth strategy with targeted acquisitions

IMPACTS & ACHIEVEMENTS

For our employees

- **145** e-learning trainings available to all employees
- **112 employees** enrolled in the *RiseUp* Top Talents programme
- Strong engagement score : **66 %**

For our partners and clients

- **Reseller NPS**: 48 in 2024 (EMEA), highlighting solid satisfaction
- **20,000** tickets in Europe
- Financing support: solutions + XPS offer
- **+11,000 partners** and customer trained in cybersecurity
- Integrity due diligence performed on **+ 20 000 third parties**
- **1 500 tons** of hardware freight transported

For society and the planet

- **40%** reduction in scope 1 and 2 emissions by 2030
- **85%** employees certified the Code of Conduct
- **Low Cyber Exposure Score (CES)** for the third consecutive year
- Certificates **EcoVadis, CDP, ISO 9001 & ISO 14001 (UK), ISO 27001 (Group)**



For our shareholders

#VALUE!



VISION

A fully reliable digital world, made more secure by the most innovative technologies.

Who We Are

Exclusive Networks is a global cybersecurity specialist and go-to-market partner, connecting the world's leading cybersecurity technology vendors with a network of more than 20,000 reseller partners and, through them, with end-users ranging from large enterprises to small and medium-sized businesses. Headquartered in Boulogne-Billancourt, France, the Group operates as a value-added distributor (VAD): rather than manufacturing hardware or software itself, Exclusive Networks' role is to make the world's most advanced cybersecurity solutions accessible, deployable and effectively supported, from pre-sales technical advisory through to post-sales training, managed services and customer success.

The Group's mission is to be the leading trusted global cybersecurity go-to-market specialist, contributing to the transition to a trusted digital future for people and organizations worldwide. This positions Exclusive Networks at a distinctive point in the cybersecurity value chain: not as a producer of technology, but as the specialist infrastructure – logistics, technical expertise, financing, training and local market access – that determines how effectively that technology reaches and protects the organizations that need it.

Scale and Footprint

As at 31 December 2025, Exclusive Networks employed 3,102 people (up 7% from 2,895 in 2024), organized across three macro-regions, EMEA (70% of the workforce), APAC (23%) and the Americas (5%), with a presence spanning 50 countries and logistics or service capability reaching more than 170 countries served. The Group's portfolio covers all major cybersecurity segments, network, endpoint, cloud, identity and data security among them, built on partnerships with category-leading vendors such as Fortinet, Palo Alto Networks, F5, SentinelOne and Proofpoint, and extended in 2025 through a new strategic distribution agreement with Amazon Web Services (AWS) across the European Economic Area and Switzerland.

Growth has come through both organic expansion and disciplined M&A: more than 20 acquisitions over the past decade, including, in July 2025, the acquisition of DAN Distribution, extending the Group's footprint into Estonia, Latvia and Lithuania. Specialist brands within the Group, such as Ignition Technology, extend this reach into complementary and emerging areas of the cybersecurity market.

A Company in Transition

FY2025 was a year of structural change as much as operational growth. In March 2025, a consortium formed by CD&R, Permira and founder Olivier Breittmayer completed the acquisition of Exclusive Networks; the squeeze-out procedure closed on 21 March 2025 and the transaction completed on 24 March 2025, at which point the Group was delisted from Euronext Paris and became a privately held company. This was followed in April 2025 by an evolution of the Group's leadership and operating structure under CEO Jesper Trolle, designed to support the next phase of growth, vendor diversification and services expansion.

This transition matters for how this report should be read. Exclusive Networks is no longer subject to the mandatory disclosure obligations that apply to listed companies, including, at present, the Corporate Sustainability Reporting Directive (CSRD). The Group has nonetheless chosen to continue, and to deepen, its voluntary alignment with the European Sustainability Reporting Standards (ESRS), building on the reporting discipline, double-materiality process and external assurance practice it established as a public company. This report is the clearest expression of that choice: a voluntary, ESRS-structured disclosure, independently reviewed by KPMG, published because the Group considers robust, comparable ESG reporting integral to how it operates and to the trust of its vendors, partners, employees and shareholders.

Why Sustainability Is Structural, Not Peripheral, to This Business

As a distributor rather than a manufacturer, Exclusive Networks' direct environmental footprint, its own offices, vehicles and energy use, is comparatively modest. The Group's real sustainability leverage sits elsewhere: in the value-chain emissions embedded in the products it moves through global logistics networks (the great majority of its carbon footprint), in the integrity and resilience of a global, multi-country workforce, and, distinctively for a cybersecurity distributor, in the societal role its core business already plays. Every transaction the Group enables enhances the protection of data, infrastructure and users against a growing volume of cyber threats; secure digital access is not a side effect of what Exclusive Networks does, it is what Exclusive Networks does.

This report sets out, transparently and against measurable targets, how the Group manages both sides of that equation: the footprint it creates in doing business, and the protective impact that business has on the wider digital economy.

2 Sustainability strategy 2024–2030

2.1 Cybersecurity as an enabler of sustainability

Exclusive Networks' sustainability strategy starts from the Group's core activity: enabling the secure adoption of digital technology.

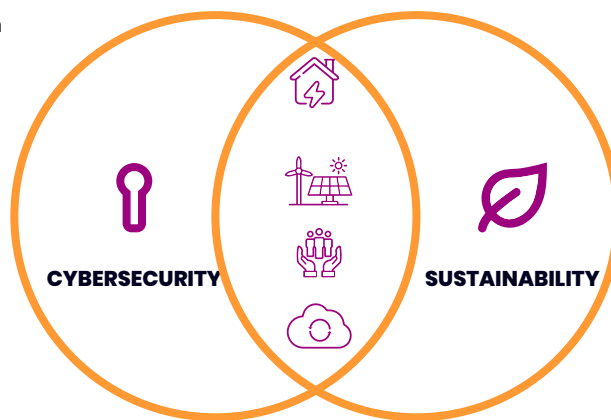
As organisations accelerate their use of connected devices, cloud infrastructure and renewable-energy systems, the security of these technologies becomes a precondition for their contribution to broader environmental and social goals. Exclusive Networks views its role as a distributor of cybersecurity capability as directly supporting that precondition, across four areas of intersection between digital transformation and sustainability:

SMARTIFICATION³

the growth of interconnected devices increases the surface area that must be secured for digitalisation to deliver its efficiency benefits rather than new sources of risk.

ENERGY TRANSITION¹

secure operational technology and IoT deployments underpin the reliability of renewable-energy and smart-grid systems.



SOCIAL EQUITY⁴

smaller organisations are disproportionately exposed to cyberattacks and their consequences; extending affordable, effective security to this segment is a social as much as a commercial objective.

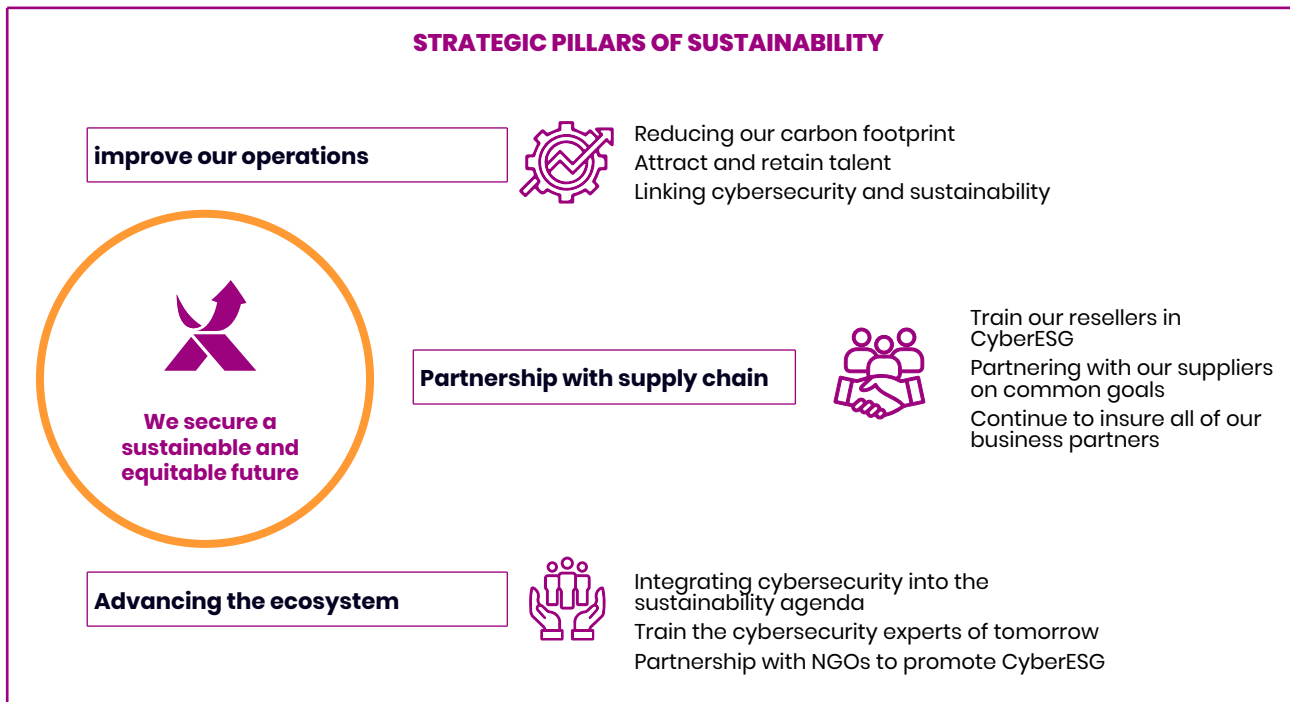
CLOUD ADOPTION²

the shift toward cloud-based infrastructure depends on trust in the security of that infrastructure to be sustained at scale.

These four areas frame why Exclusive Networks treats cybersecurity and sustainability as linked agendas rather than parallel ones. External market figures cited in support of this framing (IoT, cloud and cyberattack-exposure statistics) describe overall market context rather than Exclusive Networks' own performance and are sourced to the third-party research cited alongside them.

2.3 Strategic pillars

The Group's sustainability strategy rests on three pillars, unchanged from the FY2024 report and reaffirmed as the framework for the 2024–2030 horizon:



Each pillar translates into concrete commitments and metrics reported in the relevant environmental, social and governance chapters of this report, rather than being managed as a stand-alone communications theme.

2.2 Strategy development process

The Group's 2024–2030 sustainability strategy was built through a structured, evidence-based process rather than asserted top-down. Four inputs shaped the resulting strategic pillars and material-topics list:

- **International sustainability frameworks** : the Global Reporting Initiative (GRI) and the Sustainability Accounting Standards Board (SASB) supplied the initial universe of topics and disclosure language against which Exclusive Networks' own activities were screened.
- **Stakeholder engagement** : structured input from employees, vendors, resellers and shareholders was used to test which of the topics identified were genuinely relevant to the Group's business model and value chain.
- **Risk assessment and strategic business considerations** : the Group's existing risk mapping was layered onto the topic list alongside its competitive position, regulatory exposure, reputational factors, and stated purpose and strengths, to prioritise the topics most likely to affect, or be affected by, the business.
- **Internal materiality workshops** : cross-functional sessions translated the resulting, prioritised topics into the three strategic pillars set out in Section 2.3 and produced a working list of roughly twenty qualified sustainability issues mapped to the ESRS/CSRD nomenclature.

Anticipating the strategy and target refresh

Looking ahead, Exclusive Networks plans to undertake a Double Materiality Assessment (DMA) in 2026, aligned with the seven-step methodology set out in ESRS 1 and Delegated Regulation (EU) 2023/2772.

This planned refresh is voluntary. Following its take-private transaction in 2025, Exclusive Networks is not currently subject to the Corporate Sustainability Reporting Directive.

The Group intends nonetheless to conduct its double materiality assessment in line with ESRS methodology and to plan its target refresh on the same basis, in order to build a consistent, auditable reporting history ahead of any future regulatory obligation and in response to the ESG due-diligence expectations increasingly set by the Group's own vendors, financing partners and larger customers.

2.4 Initiative CyberESG

CyberESG is Exclusive Networks' new initiative that sits at the intersection of cybersecurity and the three main pillars of sustainability (Environmental, Social, and Governance).

CyberESG is about using our cybersecurity practices not only to protect against threats, but also to contribute positively to our planet, people, and ethical business practices.

CyberESG supports the strategy with four key programs:

- **Certification** : Providing employees with integrated cybersecurity and sustainability training.
- **Partner Enablement** : Help resellers adopt sustainable practices. To strengthen our commitment to sustainable practices across the digital ecosystem, we have actively engaged with key partners such as Fortinet, Palo Alto, Mimecast, CDW, NTT Data and others.

This collaboration includes:

- Joint participation in double materiality assessments to identify and prioritize key sustainability issues.
- Share our sustainability achievements and roadmap to encourage transparency and best practices.
- Contribute to industry think tanks focused on improving transparency around the carbon footprint of hardware.
- Share our expertise through guest lectures at webinars focusing on key topics such as scope 3 and CSRD.
- Ongoing dialogue and meetings to support a continuous improvement of sustainability efforts.
- **Awareness campaigns**: Engage audiences (internal and external) through social media and educational blogs.
To ensure that our entire organization is aligned with our sustainability goals, we have launched an extensive internal awareness campaign:
 - **CyberESG Pulse Newsletter**: This regular publication keeps employees informed of global sustainability initiatives, strategies and commitments across the company, fostering a shared understanding of our progress.

- **Centralized SharePoint Hub**: this platform serves as a one-stop-shop for all sustainability issues, providing FAQs (Frequently Asked Questions) , resources and materials to equip employees in their conversations with customers and partners. This resource has been directly informed by the challenges and questions raised by our clients, ensuring relevant and updated content.
- **Extend reach outside**: We have used social media to reach a wider audience and highlight our commitment to sustainable development:
 - **LinkedIn**: We shared key milestones including the launch of our SNFP, our EcoVadis score and our commitment to the Science Based Targets (SBTi) initiative.
 - **Amplifying content**: We have expanded the reach of our internal initiatives by sharing highlights from our webinars and employee engagement programs, demonstrating our organization-wide commitment to sustainability.
- **Podcast series**: Share ideas and inspire action through discussions with industry leaders.

To amplify the debate on sustainability in cybersecurity, we are developing an engaging podcast series. Featuring insightful discussions with industry leaders from our partner network, the podcast will explore key topics and inspire action. Although the series is scheduled to launch in 2026, we have already organized a compelling list of speakers and invited topics. Stay tuned for updates on this exciting initiative.

3.4 Membership requirements for the CyberESG community

All members supporting the governance framework are part of the CyberESG community.

Membership requirements include:

- Completion of internal level 1 training on sustainable development.
- Regular attendance at strategic meetings and reviews.
- Active promotion of sustainability within their departments through internal and external communication platforms.

As part of our CyberESG initiative, we have organized several virtual sustainability events to train our staff on key sustainable development trends. These sessions focused on understanding our sustainability strategy and commitments to empower our employees to better support our customers.

In order to spread the spirit of CyberESG throughout the company, we have adopted a multi-faceted communication approach:

- **CyberESG Newsletter**: Regular updates to keep employees informed and aligned with sustainability goals
- **Internal communication channels**: Frequent discussions and updates on the channel across the company to ensure ongoing engagement.
- **CyberESG Hub**: a centralised internal platform acting as the single source of truth for sustainability initiatives. It hosts the Group's certifications (**ISO 27001, covering the entire Group, and ISO 9001 and ISO 14001, covering the UK entity**), the **EcoVadis** and **CDP (Carbon Disclosure Project)**, dashboards, answers to frequently asked customer questions, and a library of sustainability documents.

These efforts have fostered a culture of awareness and commitment to sustainability within the organization.

This culture change has also strengthened our ability to proactively respond to customer sustainability demands and align internal practices with evolving ESG standards.

CyberESG Newsletter Example:



Dear colleagues,

We're excited to present the second edition of CyberESG Pulse! In our [previous newsletter](#), we discussed the fundamentals of sustainability and clarified the link between sustainability and cybersecurity.

This month, we'll further explore the **synergy between the two**, providing you with some compelling reasons for positioning Exclusive Networks as a sustainable partner of choice. Also, you'll get a sneak peek at our **first digital event** !

Internal communication channels: example interface



Welcome to **CyberESG Hub**: our internal Sustainability Hub – your comprehensive resource for understanding and advancing our company's environmental and social commitments.

Why did we call our Sharepoint CyberESG Hub?

CyberESG is the new Exclusive Networks initiative that stands at the intersection of Cybersecurity and Environmental, Social, and Governance (ESG) principles.

CyberESG is about leveraging our cybersecurity practices to not only defend against threats, but also to contribute positively to our planet, people, and ethical business practices.

This platform is designed to **equip and inform** our team, providing the knowledge and tools needed to:

- Understand our sustainability strategy
- Access critical learning resources
- Stay informed about our ESG progress
- Support our corporate sustainability objectives

3 Sustainability governance framework

Exclusive Networks has established a robust sustainability governance framework designed to ensure that sustainability is fully embedded into the Group’s strategy, decision-making processes, and day-to-day operations.

This framework supports the effective oversight, management, and integration of environmental, social, and governance (ESG) matters across the Group, in line with regulatory expectations and stakeholder expectations.

3.1 Mission

Exclusive Networks Group seeks to create lasting value for its stakeholders by embedding responsibility, ethics, and integrity into every aspect of its operations.

3.2 Governance Structure

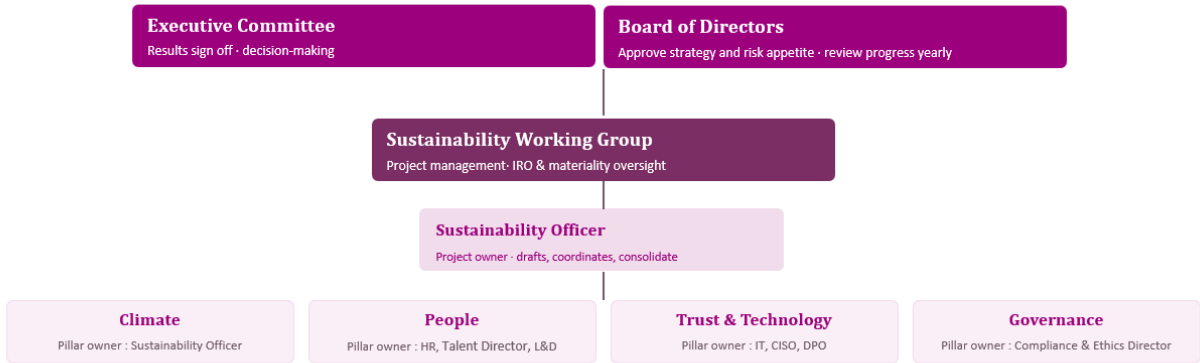
This framework supports the effective oversight, management, and integration of environmental, social, and governance (ESG) matters across the Exclusive Networks Group, in line with regulatory expectations and stakeholder expectations.

Sustainability Governance Structure

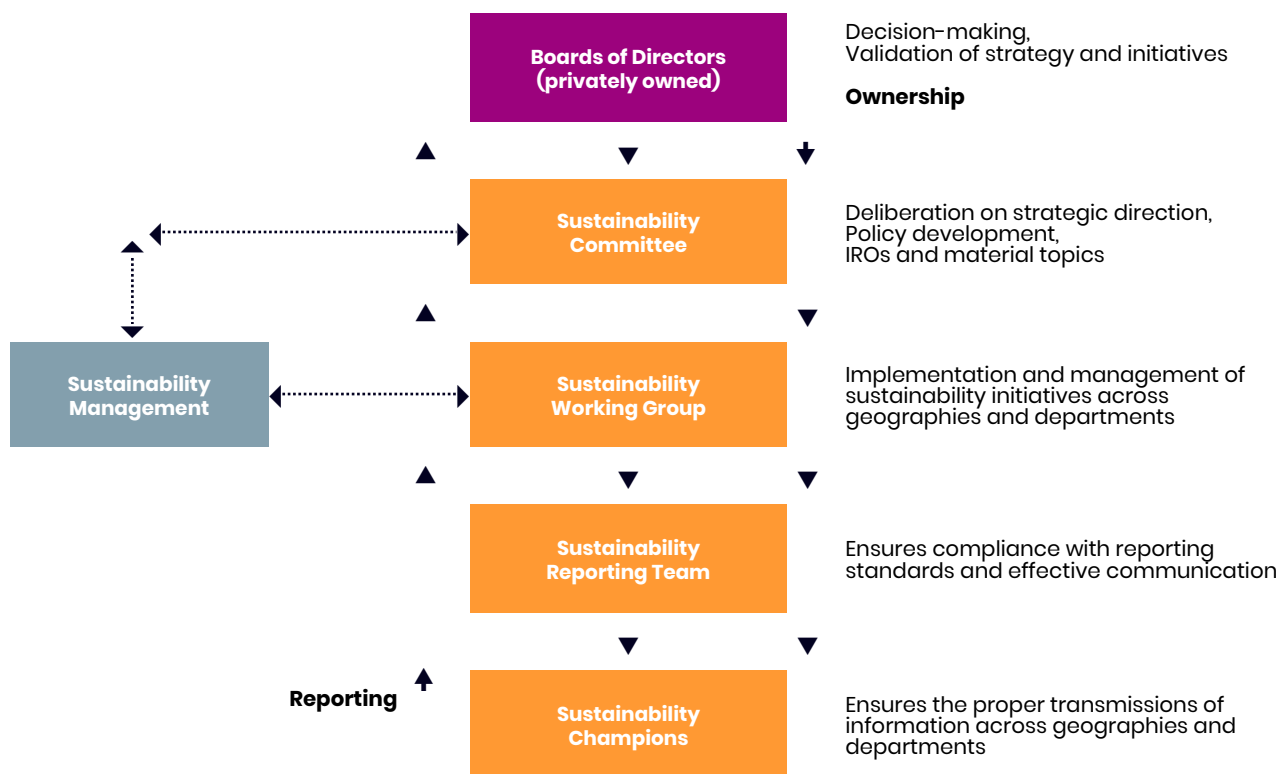
STRATEGY CORE · GOVERNANCE

Governance & Ownership Structure

Clear ownership from Board to pillar owners, with a fixed review cadence.



Sustainability governance framework



3.2.1 Governance Structure and Oversight

Following the Group's transition to private ownership in 2025, sustainability governance is integrated into Exclusive Networks' corporate governance framework and decision-making processes. The governance structure is designed to ensure the effective identification, assessment, management and monitoring of sustainability-related impacts, risks and opportunities (IROs), while supporting the Group's long-term strategy and value creation objectives.

The Board of Directors has ultimate oversight of sustainability-related matters. The Board reviews the Group's sustainability strategy, monitors material sustainability-related impacts, risks and opportunities, and considers their potential effects on the Group's business model, strategy and performance. Sustainability matters are addressed as part of the Board's broader oversight responsibilities relating to strategy, risk management and corporate governance. The Board periodically reviews progress against sustainability objectives and receives updates from management regarding significant sustainability developments and priorities.

The Executive Committee is responsible for implementing the sustainability strategy and ensuring the integration of sustainability-related considerations into business planning, operational management and decision-making processes. The Executive Committee reviews sustainability performance, evaluates progress against strategic priorities and supports the allocation of resources necessary to deliver sustainability objectives. Sustainability-related matters are discussed alongside operational, financial and strategic considerations to support informed management decisions.

The Sustainability Working Group supports the Executive Committee by coordinating the Group's sustainability programme and facilitating cross-functional collaboration. The Working Group oversees the management of sustainability-related initiatives, supports the identification and assessment of material impacts, risks and opportunities, monitors the implementation of action plans and coordinates sustainability reporting activities. The Working Group serves as the primary forum for reviewing sustainability-related matters before escalation to senior management where appropriate.

The Sustainability Officer is responsible for coordinating the implementation of the sustainability programme and reporting process. The Sustainability Officer facilitates collaboration across business functions, consolidates sustainability information, supports the monitoring of objectives and targets and coordinates the preparation of sustainability disclosures. The role also supports the management of the Group's double materiality assessment process and the monitoring of material sustainability-related impacts, risks and opportunities.

Implementation responsibilities are delegated to designated sustainability pillar owners who are accountable for managing sustainability-related topics within their respective areas of expertise and reporting progress through the governance structure:

- **Climate:** environmental performance, greenhouse gas emissions management, climate-related initiatives and decarbonisation actions.
- **People:** workforce-related matters, including talent development, diversity, equity and inclusion, employee engagement, wellbeing and learning initiatives.
- **Trust & Technology:** cybersecurity, information security, privacy, responsible technology and digital trust.
- **Governance:** ethics, compliance, anti-corruption, responsible business conduct and related governance matters.

Through this governance framework, sustainability-related impacts, risks and opportunities are monitored and reported through defined reporting lines from pillar owners to the Sustainability Officer and Sustainability Working Group, to the Executive Committee, and ultimately to the Board of Directors. This approach supports accountability, cross-functional coordination and the integration of sustainability considerations into the Group's governance, risk management and strategic planning processes.

4 Analysis of material Impacts, Risks and Opportunities (IROs)

4.1 Process for analysing double materiality

Exclusive Networks' double materiality assessment aims to identify and prioritize the sustainability matters that are most relevant to the Group and its stakeholders, considering both:

- Impact materiality, which assesses the Group's actual and potential positive and negative impact on people and the environment,
- Financial materiality, which considers sustainability-related risks and opportunities that may have a material financial effect on the Group.

The Group approach to materiality has progressively evolved since 2022, leading the double materiality assessment conducted in 2024 using the ESRS/CSRD nomenclature and produced a working list of roughly twenty qualified sustainability issues, from which the material Impacts, Risks and Opportunities (IROs) set out in this chapter were drawn.

Identification and engagement of stakeholders:

Stakeholders' engagement is an important component of the Group's materiality assessment. The stakeholder mapping established as part of the 2024 double materiality assessment continued to serve as the reference framework in 2025;

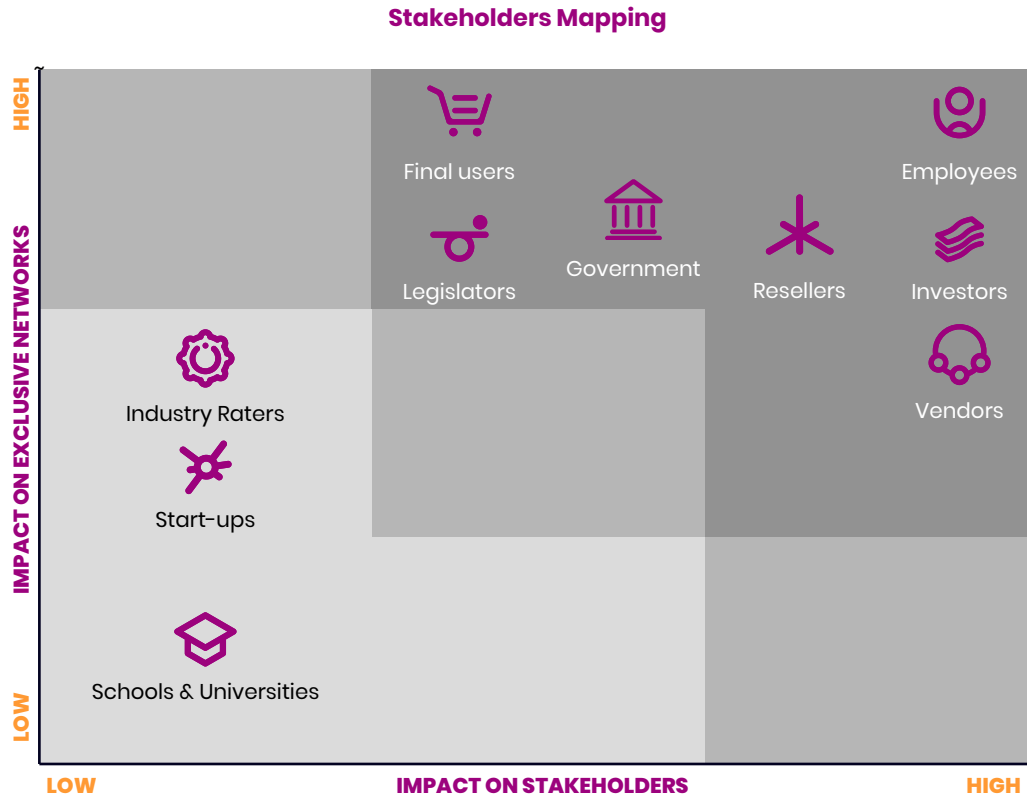
The Group key stakeholder matrix includes end-users, resellers, vendors, and other business partners, employees, regulators, investors, industry raters, start-ups, schools and universities.

The mapping enables the Group to identify the stakeholders most relevant to its activities and sustainability matters and to take their perspectives into account when assessing the Group's impact, risks and opportunities;

This gave the Group its first structured, standards-referenced view of where its business model creates impact and is itself exposed to sustainability-related risk.

Throughout 2025, the Group continued to build on the findings of its 2024 double materiality assessment, which remained the reference framework for identifying and prioritising material sustainability matters. The material topics and double materiality matrix presented below therefore provide continuity with the Group's established sustainability priorities while supporting its ongoing strategic work.

On this matrix, vendors, resellers, employees, regulators and investors sit in the high-impact, high-influence quadrant and are treated as priority engagement groups; government bodies and industry raters carry high impact on the Group but are engaged mainly through compliance and ratings channels such as EcoVadis and CDP; final users register high impact on the Group as the ultimate demand driver behind the vendors and resellers it serves; and start-ups, schools and universities currently sit lower on mutual impact, engaged principally through the Group's training and ecosystem-development activities.



During 2025, the Group initiated a review of its value chain and stakeholder mapping as part of the broader work undertaken to prepare for the new double materiality matrix assessment. This work aims to provide a more comprehensive understanding of the Group upstream and downstream activities and relationships and to identify the stakeholders group most relevant to the assessment of its sustainability impacts, risks and opportunities. EXN's value chain will be disclosed in the next Sustainability report.

2024 double materiality matrix: results

Based on the double materiality assessment made in 2024, the following topics were identified as material :

ESRS topic	Material sub-issues identified
E1 – Climate Change	Group GHG footprint, concentrated in Scope 3 value-chain emissions (see the Environmental chapter).
E5 – Resource Use & Circular Economy	Circular procurement and end-of-life management of IT and hardware equipment.
S1 – Own Workforce	Health & safety; gender equality and equal pay; work-life balance; social dialogue; training and skills development; diversity.
S1 / S4 – Privacy	Data protection and privacy, spanning both the Group's own workforce and its consumers/end-users.
G1 – Business Conduct	Corruption and bribery prevention; responsible-purchasing relationship management with suppliers.

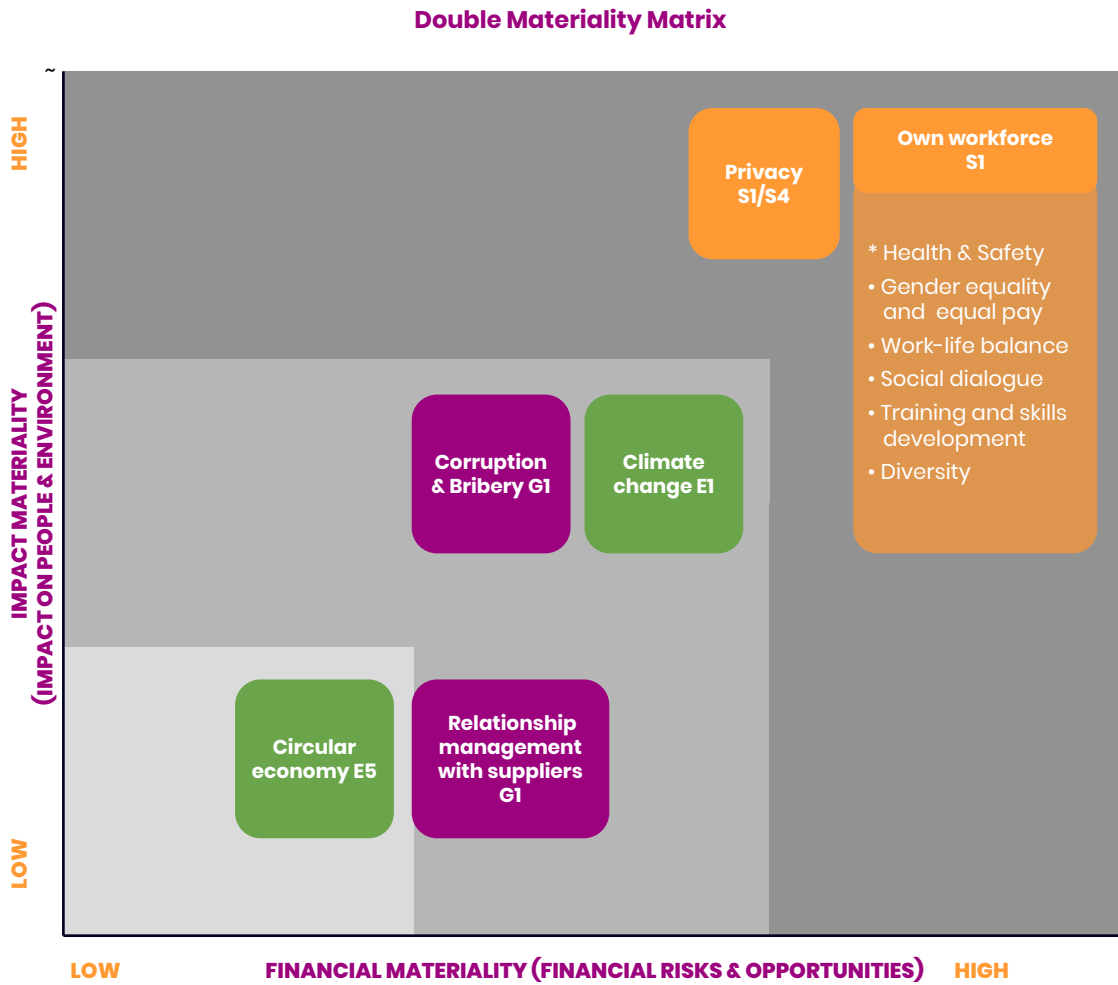
Topics screened out as non-material in 2024

Not every topic in the ESRS/CSRD nomenclature was carried through to a full double materiality analysis. The following topics (including their underlying issues and sub-issues) were screened out in 2024, for the reasons stated:

Analysis of material Impacts, Risks and Opportunities (IROs)

Topic	Reason screened out
E2 – Pollution	No direct link identified between the topic and the Group's activity as a distributor.
E3 – Water & Marine Resources	No direct link identified between the topic and the Group's activity as a distributor.
E4 – Biodiversity & Ecosystems	No direct link identified between the topic and the Group's activity as a distributor.
S2 – Workers in the Value Chain	Assessed as having limited impact on the Group, and vice versa, at the 2024 screening threshold.
S3 – Affected Communities	Assessed as having limited impact on the Group, and vice versa, at the 2024 screening threshold.

These results are presented here as a structured matrix of double materiality along the two axes. The matrix below reflects the outcome of the double materiality assessment conducted in 2024 and remained the Group's reference framework for the identification and prioritization of the material sustainable matters in 2025.



What comes next

In 2025, Exclusive Networks initiated, on a voluntary review expected to be concluded in 2026, a comprehensive review of its double materiality matrix (DMA) approach drawing on the principles, methodology and requirements of the European Corporate Sustainability Reporting Directive (CSRD) that requires certain companies to publish an annual sustainability report detailing their environmental, social, and governance (ESG) impact.

This new assessment includes a comprehensive reassessment of the Group's material impact, risks and opportunities, informed by the review of its value chain and stakeholders.

4.2 Key ESG-related risks and opportunities identified

The following table presents refined information on challenges, impacts, risks and opportunities aligned to ESG dimensions:

CHALLENGES	IMPACTS	RISKS	OPPORTUNITIES
Climate change E1	Reduced carbon footprint	Regulatory charges, carbon taxes	Adoption of renewable energy, innovations in energy efficiency
Circular Economy E5	Improving e-waste management	Increased compliance costs	CyberCircular Customer Loyalty Programs
Privacy S1 (Own workforce)	Employee and customer confidence	Violations involving legal and reputational risks	Leading position thanks to robust data protection
Diversity (St)	Innovation and labour inclusion	Attrition of talent due to lack of attractiveness	Improved capacity for innovation through diverse teams
Supplier relationship (G1)	Resilient and ethical supply chains	Supplier disruptions	Stronger ESG profiles and shared value creation
Corruption and bribery (G1)	Ethical differentiation of reputation	Legal, reputational and operational risks	Building trust with partners and customers

5 Exclusive Networks' sustainability commitments

Exclusive Networks is strongly committed to sustainability by integrating environmental, social and governance (ESG) principles into all aspects of its operations. Guided by our strategic pillars, we continuously strive to mitigate risks, leverage opportunities and make positive changes for our stakeholders.

5.5 Roadmap to address sustainability issues

Pillars of our strategy	Material Topics ESRS Mapping*	Our Commitments	Actions	Progress	
				2022	2025
 Improve our operations 	Comprehensive Talent Management * ESRS : Social Dialogue, Balance between professional life and Privacy, Health & Safety, Gender Equality and Gender Equality Remuneration for work of equal value, Training and development of Skills, Diversity	Increase our employee engagement rate from 72% to 77% by 2025, base year 2022 Increase the % of women in senior management roles from 34% to 40% by 2025, base year 2022	Develop a Performance Culture built on : Clear recognition based on employees' performance Education Feedback culture and proper onboarding Monitor the Diversity ratio for Management roles	72 %	66%
	Ethics * ESRS : Corruption & Bribery	Train 100% of employees on DE&I and Ethics by 2025, base year 2022	Implement trainings and certification Programmes	NA	DE&I 79 % Ethics 100 % (2024) Sustai. NA
	Cybersecurity * ESRS : Privacy	Reduce our Cyber Exposure Score from Medium to Low by 2025	Additional SOC reporting to address vulnerabilities Weekly meetings to identify vulnerabilities Collaboration with Digital Workplace team	Medium	Low
	Energy Management/ Scope 1-2 * ESRS : Climate change	Reduce absolute Scopes 1 & 2 GHG emissions by 40% by 2030	Switch to Electric or Hybrid of Vehicles , Switch to Renewable Energy of Electricity use Upgrade in Energy efficiencies in operations Implement Energy Management Systems		New base year
	Product Lifecycle Management * ESRS : Circular Economy	Recycle 100% of end-of-life products by end of 2030	Circular Procurement Strategies	NA	NA
 Partner with supply chain 	Energy Management/ Scope 3 * ESRS : Climate change	Reduce scope 3 emissions per unit of income by 33% in 2030	Supplier Engagement for Sustainable Practices Optimize Logistics Product Redesign for Efficiency Remote Working and Public Transport Incentives		New base year
	Export Control * ESRS : Management of Relationship with Suppliers	Ensure the integrity of 100% our Business Partners by 2023	Digital Partner Onboarding mandatory	4,968	21,128
 Advance the ecosystem 	Human Resource Adequacy and Capability * ESRS : Training & Skills Development	Reduce the skills gaps in the cybersecurity sector		11 163 people trained	13,627 people trained

6 Environmental Information

Environmental matters are an integral part of Exclusive Networks' sustainability strategy and overall governance framework. While the Group is not yet subject to mandatory reporting under the Corporate Sustainability Reporting Directive (CSRD), it has chosen to progressively align its environmental practices and disclosures with the European Sustainability Reporting Standards (ESRS) in order to anticipate future reporting obligations, currently expected to apply from FY 2027. Reported environmental topics are identified through the Group's materiality assessment and reflect key environmental impacts, risks and opportunities related to its activities and value chain performed in 2024.

In 2025, the Group undertook a comprehensive restructuring of its carbon calculation approach to improve the reliability, consistency and traceability of

greenhouse gas emissions data. This initiative aimed to strengthen methodologies, internal processes and controls, and to align carbon accounting practices with recognised international frameworks, in particular the Greenhouse Gas (GHG) Protocol, as well as with the principles underpinning future CSRD-compliant reporting.

This restructuring was supported by enhanced collaboration with external experts and key partners across the value chain, reflecting the Group's exposure to indirect emissions and its commitment to continuously improving the quality of environmental data. These efforts form part of a long-term sustainability roadmap and are not impacted by ongoing regulatory discussions, including the Omnibus package, nor by any phasing-out of sustainability ambitions.

6.1 Governance of environmental questions

Environmental matters are integrated into the Group's sustainability management and reporting processes. Responsibility for environmental topics is assigned to the relevant functions and topic owners, including those responsible for environmental performance, greenhouse gas emissions, climate-related initiatives and decarbonisation actions.

These functions support the implementation of environmental actions, the monitoring of environmental performance and the collection of environmental data.

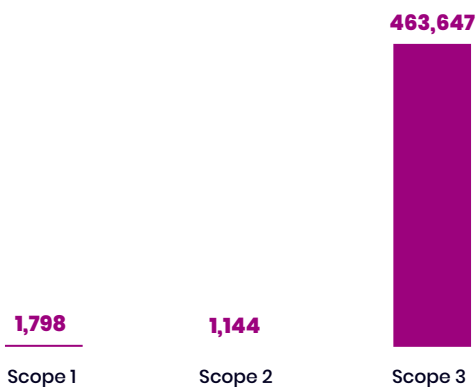
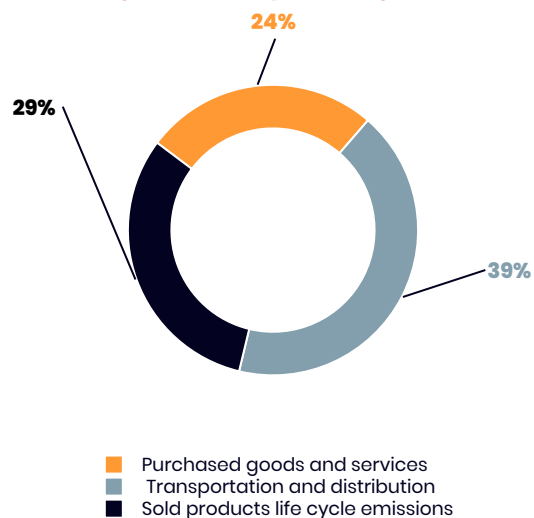
Environmental impacts, risks and opportunities identified through the Group's materiality assessment are monitored as part of the Group's sustainability management processes and reporting activities. Environmental information is subject to review and consolidation procedures designed to support the completeness, consistency and reliability of disclosed information, which is also third party audited.

6.2 Climate Change

Carbon Footprint

In 2025, we enhanced the way we calculate our carbon footprint, demonstrating our renewed dedication to addressing climate change and our resolve to implement a broader, more transparent strategy. Consequently, 2025 now serves as the baseline year for our targets to reduce greenhouse gas emissions.

	Retrospective data		Milestones and target years				
	Base year	Ref year data	N	% N/N-1	2026	2030	-2050 Annual target in % / base year
Scope 1 GHG emissions	2025	2025					
Scope 1 GHG emissions (tCO ₂ eq)		1,798					
Percentage of Scope 1 GHG emissions from regulated emissions trading systems (%)							
Scope 2 GHG emissions							
Market-based Scope 2 gross GHG emissions (tCO ₂ eq)							
Gross Scope 2 Location-Based GHG Emissions (tCO ₂ eq)		1,144					
Significant scope 3 GHG emissions							
Total gross indirect GHG emissions (scope 3) (tCO ₂ eq)		463,647					
Cat. 1 Purchased goods and services [Optional Subcategory: Cloud Services & Data Centre]		109,552					
Cat. 2. Capital Assets		0					
Cat. 3. Fuel- and energy-related activities (not included in S1 and S2)		894					
Cat. 4 Upstream transportation and distribution		180,812					
Cat. 5 Waste generated in operations		348					
Cat. 6. Business travels		82					
Cat. 7. Employees commuting		35,219					
Cat. 8. Upstream Leased Assets		0					
Cat. 9. Downstream transportation and distribution		671					
Cat. 10. Processing of Sold Products		0					
Cat. 11. Use of Products Sold		71,156					
Cat. 12. End-of-life treatment of sold products		64,913					
Cat. 13. Downstream Leased Assets		0					
Cat. 14. Franchises		0					
Cat. 15. Investments		0					
Total GHG emissions		466,589					

Share of CO₂ emissions by scope 2025
(tCO₂e)CO₂ emissions distribution across the most significant Scope 3 categories

Performance overview

Scope 3 emissions represent the vast majority of Exclusive Networks' greenhouse gas emissions footprint, reflecting the nature of the Group's business model as a value-added distributor of third-party technology products and services. The principal sources of emissions arise from upstream activities within the value chain, including the manufacture of purchased products, transportation and distribution activities, and other indirect emissions associated with suppliers.

Scope 1 and Scope 2 emissions, primarily associated with office operations and company vehicles, constitute a comparatively smaller proportion of the Group's total emissions footprint.

During fiscal year 2025, Exclusive Networks continued to strengthen the quality and completeness of its greenhouse gas inventory through enhanced engagement with suppliers and vendors. Efforts focused on improving the availability of primary data, supporting product life-cycle assessments, and refining emission calculation methodologies across relevant Scope 3 categories.

The Group's climate-related transition risks are predominantly associated with its value chain emissions. Given that the majority of emissions occur outside the Group's direct operational control, progress towards long-term emissions reduction objectives depends on factors including supplier emissions-reduction initiatives, the availability of reliable emissions data, developments in low-carbon technologies, and evolving regulatory and market conditions.

To address these challenges, Exclusive Networks continues to collaborate with suppliers, logistics providers and technology vendors to improve emissions transparency, strengthen data quality and encourage the adoption of lower-carbon products, services and operational practices. These partnerships support the Group's climate strategy and contribute to the management of material climate-related risks and opportunities across the value chain.

Decarbonisation strategy

Exclusive Networks' decarbonisation strategy is structured around a dynamic and continuous process of analysis, adaptation, implementation and monitoring. This iterative approach ensures that climate-related actions remain aligned with the Group's evolving business model, operational realities and long-term sustainability objectives.

1. **Environmental impact assessment and scenario analysis** : The Group conducts an environmental impact assessment supported by scenario analysis to anticipate climate-related risks and opportunities and to design proportionate and targeted responses. Scenario analysis is used as a strategic tool to assess the resilience of the business model under different transition pathways and to inform decision-making over multiple time horizons.
2. **Implementation of mitigation measures** : The implementation phase translates strategic orientations into concrete actions across business functions. Key mitigation measures include: electrification of the vehicle fleet, optimisation of supply chain and logistics flows, limitation of business air travel, improvement of energy efficiency in facilities, and the increased use of recycled materials. These measures are deployed progressively and embedded within operational processes to ensure effective execution.
3. **Monitoring and follow-up** : Progress is monitored through regular reviews against defined milestones, notably the 2025 and 2030 targets. This follow-up mechanism enables the Group to assess performance, identify deviations and adjust actions as necessary to remain aligned with its decarbonisation pathway.

Environmental scenarios

Exclusive Networks has defined two environmental scenarios to frame its decarbonisation journey and assess potential trajectories over time.

Business-as-usual (BAU) scenario

Environmental Information

The business-as-usual scenario assumes the continuation of current economic and market trends without additional constraints linked to climate objectives. This scenario is characterised by:

- continued growth in the cybersecurity market, with Exclusive Networks anticipating market expansion to approximately USD 106 billion by 2027;
- a stable balance between hardware and cloud solutions, resulting in increased energy consumption linked to hardware products.

Under this scenario, no significant additional actions are undertaken by the Group or external stakeholders to alter the existing emissions trajectory

Transition Scenario (T)

In contrast, the transition scenario describes a proactive alignment with a lower-carbon business model, driven by macroeconomic developments, regulatory signals and stakeholder actions.

While sales follow a similar growth trajectory to the BAU scenario, this pathway assumes a progressive shift toward a greater share of services and software solutions by 2030, supported by energy efficiency improvements delivered by suppliers.

This scenario combines:

- internal actions, such as fleet electrification, reduced air travel, freight optimisation and increased use of recycled plastics; and
- external factors, including the decarbonisation of national energy mixes, supplier commitments to

energy efficiency and regulatory measures such as restrictions on coal-based urban heating networks in France.

The transition is assumed to be facilitated by increasing environmental awareness and supplier-led efficiency improvements across the value chain.

These scenarios are not intended as forecasts but as strategic tools to navigate transition risks, capture opportunities and support the development of the Group's 2024–2030 decarbonisation roadmap. Recent initiatives have contributed to stabilising absolute emissions despite revenue growth, notably through renewable energy adoption and product re-engineering efforts.

The Group considers multiple time horizons in its sustainability and climate-related disclosures to reflect both operational needs and longer-term strategic objectives:

Time horizons considered :

- a short-term horizon, focused on annual performance monitoring and the 2025 reporting year; and
- a medium-term horizon, aligned with 2030 milestones and the implementation of the decarbonisation roadmap.
- the long-term horizon refers to a period beyond 2030.

These time horizons support a structured and forward-looking approach to climate strategy and performance management.

6.2 Methodological note

This methodological note sets out the approach used by Exclusive Networks to calculate and report its greenhouse gas (GHG) emissions for the 2025 reporting year. Its purpose is to ensure transparency, consistency, and comparability of emissions data over time, in line with internationally recognised standards and evolving regulatory expectations.

The carbon footprint has been prepared in accordance with the GHG Protocol Corporate Accounting and Reporting Standard, which serves as the primary reference framework for defining organisational boundaries, classifying emissions by scope, and applying core calculation principles. Emissions are expressed in metric tons of carbon dioxide equivalent (tCO₂e), using recognised global warming potentials (GWPs) to enable comparability across greenhouse gases.

Data collection and calculation processes draw on a hybrid approach combining primary and secondary data. To strengthen data quality and reliability, Exclusive Networks works in close collaboration with its principal suppliers to refine the emissions factors associated with purchased goods and services. The methodology, underlying assumptions, and calculation choices are fully documented to ensure traceability and auditability, in support of continuous improvement over time.

The sustainability statement encompasses the Group's own operations as well as selected stakeholders across its upstream and downstream value chain, where material impacts, risks, or opportunities have been identified. Upstream stakeholders primarily include key technology vendors and original equipment manufacturers (OEMs), logistics and transportation providers, and other strategic suppliers involved in the sourcing, distribution, and delivery of products and services.

Primary data obtained from suppliers and other value-chain partners account for approximately 78% of total Scope 3 GHG emissions

Downstream stakeholders comprise mainly customers, including resellers, integrators, and end-user organisations, as well as the end-users of distributed solutions. Value-chain coverage remains partial, reflecting the current maturity of data availability and stakeholder engagement processes.

Identification of metrics

Environmental metrics drawing on indirect upstream and/or downstream value-chain data include Scope 3 GHG emissions, calculated using sector-average emissions factors and proxy data where primary supplier data is unavailable. Any such use is specified in the relevant sections.

Basis of preparation, accuracy, and improvement actions

These metrics rely on secondary data and estimation assumptions, which inherently result in a lower degree of accuracy than direct measurement. Accuracy is expected to improve progressively as supplier engagement deepens and the use of primary value-chain data increases.

Although the Group is not yet subject to mandatory reporting under the Corporate Sustainability Reporting Directive (CSRD), it has chosen to voluntarily align its climate-related disclosures with the European Sustainability Reporting Standards (ESRS), including ESRS E1 on Climate Change, as part of a forward-looking approach to anticipate future regulatory requirements and reinforce the robustness of its sustainability reporting.

6.2.1 Scope of consolidation

Organisational boundary and consolidation perimeter

The scope of the present GHG emissions report for the 2025 financial year (1/01/2025 – 31/12/2025) covers the 50 countries where the Group entities operate and represent the 100% of the Group's consolidated revenue and total workforce. They are listed below:

Australia, Austria, Belgium, Bosnia & Herzegovina, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Kenya, Latvia, Lithuania, Saudi Arabia, Malaysia, Mauritius, Morocco, Netherlands, New Zealand, Norway, Philippines, Poland, Portugal, Qatar, Romania, Serbia, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Thailand, Turkey, United Arab Emirates (Dubai), United Kingdom, United States, and Vietnam.

The consolidation scope is applied consistently across all environmental, social and governance information, including the greenhouse gas emissions inventory under the three Scopes.

Any exclusions from the reporting perimeter are justified on the basis of demonstrated non-materiality, in accordance with the principles of the GHG Protocol.

Greenhouse gas emissions considered

Greenhouse gas (GHG) emissions considered are calculated and reported in accordance with the GHG Protocol and include:

- Scope 1: direct emissions from sources owned or controlled by the Group;
- Scope 2: indirect emissions from purchased electricity and energy, calculated using the location-based approach;
- Scope 3: other indirect emissions occurring across the value chain.

Emissions are reported in metric tons of CO₂ equivalent (tCO₂e) using recognized global warming potentials to ensure comparability across greenhouse gases.

All material Scope 3 categories have been assessed and reported where data are available and sufficiently reliable, in line with the Group's materiality assessment and ESRS E1 requirements.

Emission intensity indicator on headcount

150 (tCO₂e / employee)

6.2.1 Carbon footprint methodology

Environmental information is prepared using the best available data at the reporting date and in accordance with recognised methodologies, including the GHG Protocol and emission factors sourced from authoritative databases. Where primary activity data are not available for the full reporting perimeter, estimates and extrapolations are applied using documented assumptions and historical information in order to ensure comprehensive coverage of the Group's operations and value chain. The methodology is applied consistently across the reporting perimeter and over time to support comparability of results.

Certain indicators are subject to inherent measurement uncertainty resulting from the availability and quality of underlying data, the use of modelling assumptions, and the reliance on external datasets and emission factors. These uncertainties do not affect the suitability of the information for understanding the Group's environmental impacts but may influence the precise magnitude of reported values.

The Group seeks to improve the reliability and granularity of environmental data on an ongoing basis through enhanced data collection processes, increased use of primary supplier information, and strengthened internal controls. Methodological refinements may be introduced over time where they improve the accuracy and robustness of reported information; where material, such changes are disclosed to maintain transparency and comparability.

In 2025 the methodological improvements have been primarily focused on:

- the development of a dedicated carbon calculator, based on product-level life-cycle data and validated manufacturer inputs, marks a major enhancement compared to previous estimation approaches.
- Similarly, emissions related to distribution activities have been calculated using real-world logistics data extracted directly from operational systems, ensuring a high degree of reliability for a category that reflects the core activity of the Group.

Overall, the 2025 methodology provides a robust baseline for future emissions tracking, target setting, and decarbonisation planning, while embedding a clear pathway for continuous improvement in the coming years.

The Group is not subject to the reporting requirements of the Corporate Sustainability Reporting Directive (CSRD). In preparing its climate-related disclosures, the Group has nonetheless drawn on certain principles and presentation structures of ESRS EI Climate Change, as part of a forward-looking approach intended to strengthen the robustness of its reporting. This approach does not constitute a claim of compliance with the ESRS, and not all ESRS EI disclosure requirements are covered.

General information on data collection :

- Scope 1 and 2 consumption data are centrally collected from local country contacts (typically country CFOs or finance representatives) using a standardized Excel template.

- Primary activity data (energy, fuels, travel expenses) are consolidated centrally, with follow-up clarifications performed where needed.
- Validated data are stored on the Workiva platform to ensure traceability and transparency.
- Group-level data (e.g. business travel, cost of services, and others) are sourced from validated central tools.
- Actual data are used where available; otherwise, estimates or extrapolations are applied in line with reporting principles.

Emission factors

Emission factors are selected in accordance with GHG Protocol principles, prioritising relevance, accuracy, completeness, and temporal representativeness, and ensuring appropriate scope and geographical coverage.

- Factors are primarily sourced from recognized public databases, including ADEME Base Carbone® / Base Empreinte, DEFRA, and Our World in Data, using the most recent versions available at the time of calculation.
- For product-specific emissions, manufacturer-provided data (e.g. Environmental Product Declarations) are used where available, in line with the GHG Protocol hierarchy favouring activity- and supplier-specific data.

Extrapolations

A hierarchical estimation approach was applied, prioritising same-country reference data, with building surface area (m²) used as the main allocation key.

- Where current-year data were unavailable, a standard 5% uplift was applied to prior-year local data.
- In the absence of local data, comparable-country data were used, based on geographical proximity, climatic similarity and similar operational profiles.
- Where operating data are incomplete, additional benchmarks and averages are applied, including the ADEME "Éco-responsable au bureau" (2022) benchmarks for office waste and water consumption.

Scope 1

Scope 1 emissions include all direct GHG emissions arising from sources owned or controlled by Exclusive Networks, in line with the GHG Protocol.

- Stationary combustion (S1.1): Emissions mainly result from natural gas and fuel consumption in buildings used for office activities. No renewable fuels are included in this category.
- Mobile combustion (S1.2): Emissions arise from fuel consumption of owned and leased vehicles, including diesel and gasoline vehicles used for business purposes. Electric vehicles are monitored but do not generate Scope 1 emissions.

ADEME : Gazole routier (1 litre, scope autranger) = 3,04
ADEME Essence/E85 (litre, contenance) = 2,70

- **Fugitive emissions (S1.4):** Fugitive emissions are primarily related to refrigerant leakage from HVAC systems. These emissions are considered non-determinant relative to total emissions and are estimated using standardized assumptions (capacity of 10 kW, typically serving ~110 m² of commercial spaces, using ~3 kg of refrigerant (industry standard for 10 kW systems) and global warming potentials (2088).

Scope 2

Scope 2.1 emissions include indirect greenhouse gas (GHG) emissions from purchased electricity consumed in operational sites and electric vehicles under the Group's control.

Scope 2 emissions are calculated using the location-based approach, in accordance with the GHG Protocol Corporate Standard, reflecting the average emission intensity of the electricity grids where consumption occurs.

Actual electricity consumption data derived from energy bills are used whenever available. Where data are incomplete, extrapolations are applied using a documented hierarchical approach based on local, historical, or comparable-country data, in line with recognized reporting principles.

To improve geographical granularity for electricity consumption in buildings, country-specific emission factors from Our World in Data are applied. These factors are adjusted with an additional uplift of 0.25 to account for upstream emissions associated with electricity generation, reflecting a life-cycle perspective.

For electric vehicles, ADEME emission factors are used, applying European or worldwide factors as appropriate to the geographical context.

Scope 3

Scope 3 emissions represent the largest share of the Exclusive Networks Group's greenhouse gas footprint. The most significant contributions arise from the life-cycle impacts of sold products, which account for the 53% of total Scope 3 emissions. These emissions are distributed across the product life cycle, with 43% generated upstream, 30% during the use phase, and 27% at end of life.

In light of this materiality, significant methodological improvements were implemented in 2025 to strengthen the accuracy and robustness of Scope 3 carbon estimation related to products and their commercialisation. These improvements focus on the most impactful Scope 3 categories, namely: S3.1 Purchased Goods and Services, S3.4 and S3.9 Upstream and Downstream Transportation and Distribution, S3.11 Use of Sold Products, and S3.12 End-of-Life Treatment of Sold Products. The enhanced approach reflects a life-cycle perspective and aims to improve data quality, representativeness, and consistency across the value chain.

Assumption on sold products (Categories 3.1, 3.11 and 3.12)

Exclusive Networks distributes a large and diverse hardware portfolio, comprising more than 25,000 products. While sales volumes can be reliably identified by product and by country, the availability and consistency of product life-cycle data remain limited due to fragmented supplier databases, heterogeneous data formats, and varying levels of accessibility. As a result, it is not currently practicable to assess the full life-cycle impacts of each individual product sold.

To address these data constraints, a representative sampling approach was adopted. A sample of 10 best-selling hardware products per product family was selected to reflect the main technical characteristics and sales volumes of the overall portfolio. For each selected product, a life-cycle emission calculator was developed, based on technical characteristics extracted from product data sheets (including average energy consumption) and emission factors derived from Environmental Product Declarations (EPDs) provided by manufacturers.

To ensure coverage of total hardware sales volumes, the results obtained for the representative sample were extrapolated using a revenue-based allocation, assuming that the sample collectively represents 100% of hardware sales. This approach applies to Scope 3 Categories 3.1 (Purchased Goods and Services), 3.11 (Use of Sold Products) and 3.12 (End-of-Life Treatment of Sold Products).

Life cycle phase	kgCO ₂ e/ tonne.km	Scope 3 category
Upstream (material supply, transport, manufacturing)	103447.43	3.1 (Purchased Goods and Services),
Use phase	71155.55	3.11 (Use of Sold Products)
End of life	64912.82	3.12 (End-of-Life Treatment of Sold Products)

By contrast, Scope 3 Categories 3.4 and 3.9 (Upstream and Downstream Transportation and Distribution) are excluded from this assumption and are calculated using actual logistics and transport data, ensuring alignment with real operational flows.

This methodology enables a robust and proportionate estimation of product-related emissions where granular data are not fully accessible, while also providing a replicable framework for future reporting years, supporting comparability over time.

- **Residual 3.1 Sold products and services**
 - **IT products used in operations :** IT products include individual devices assigned to employees (such as laptops, mobile phones and screens) and shared office equipment. Due to decentralised procurement practices and a Group-wide software migration in 2025, raw procurement and user-account-based data did not provide a reliable basis for identifying newly purchased devices, creating a risk of overestimation. To address these limitations, an estimation approach aligned with the Group's IT policy was applied, based on a three-year replacement cycle for individual devices. In the absence of centralised purchase records, it was therefore assumed that one-third of the total IT equipment in use corresponds to devices purchased during the reporting year. ADEME emission factors were applied.
 - **Services :** The following service-related expenditures were included : insurance, consulting, banking, legal, accounting, tax and payroll fees, recruitment, marketing and advertising, and training and converted into greenhouse gas emissions using spend-based emission factors from ADEME, based on data extracted from the Group's accounting systems.

- 3.4 & 3.9 Transportation and distribution : Upstream transportation and distribution emissions were calculated exclusively using actual logistics data extracted from the Group's internal logistics systems, reflecting Exclusive Networks' core activity as a distributor.

A dedicated emissions calculator was developed to model four distribution leg, covering transport from manufacturing sites to departure airports, international air freight, inbound delivery to Group warehouses, and outbound delivery to customers.

A granular analysis showed that air freight (airport-to-airport) represents more than the 99% of the distribution-related emission intensity, while first- and last-mile road transport have a negligible impact and were therefore excluded from product life-cycle calculations.

Emissions were calculated by matching cleaned shipment data (covering more than 2.2 million units, 17,600+ SKUs and 94 destination countries) with distance-based emission factors from ADEME Base Carbone®.

Air freight EF label : Cargo aircraft/Over 100 tons, 2023/WITH drag	kgCO₂e/tonne.km
Very short haul : <500 kms	2.83
Short haul : 500 – 1000 kms	2.98
Medium haul : 1000 – 2000 kms	2.86
Long haul : 2000 – 5000 kms	1.22
Very long haul : >5000 kms	1.01

Road freight EF label : Rigid, 3.5 to 7.5 T, on-road diesel, 7% biodiesel, Continental France, Carbon Base	kgCO₂e/tonne.km
Rigid, 3.5 to 7.5 T, on-road diesel, 7% biodiesel, Continental France, Carbon Base	0.0578

- 3.3: Fuel-and energy-related activities not included in scope 1 or scope 2 : this category includes upstream greenhouse gas emissions associated with the extraction, production and transportation of non-renewable energy sources (electricity and fuels) consumed in the Group's operations, which are not already accounted for under Scope 1 or Scope 2.
- 3.5 Waste generated in operations :
 - Waste-related emissions (office waste and WEEE) were calculated using ADEME end-of-life emission factors, and where primary data were missing or inconsistent, waste quantities were estimated using the ADEME "Éco-responsable au bureau" (2022) benchmark of 130 kg of waste per employee per year, allocated 75% to paper/cardboard and 25% to residual waste.
ADEME EF : WEEE) 2,00E+03 kg éq. CO₂/tonne de déchets, others.
 - Similarly, for water use in the office, the benchmark suggested a 10L per employees per day, to which DEFRA emission factor was applied (0,19130 kg CO₂e).

- 3.6 Business travels : Business travel emissions were calculated based on actual travel data extracted from the Navan booking tool implemented in 2025 (covering flights, trains, rental cars and hotels), consolidated by country and matched with DEFRA emission factors, with supplementary data from local travel agencies included where relevant, given the recent implementation of the tool in the year 2025.

Flight type	Economy	Premium economy	Business	First
Short (<3,700 km)	0.123	0.223	0.19	0.23
Long (>3,700 km)	0.117	0.19	0.33	0.47

- 3.7: Employee Commuting : The estimation of employee commuting relied on the average distance travelled per person each day, categorized by the mode of transport—car, train, bus, motorcycle, or bicycle—based on responses from a thorough employee survey. A 17% response rate enabled extrapolation to the broader workforce, which helped to minimize uncertainty relative to last year. This approach was applied across all the 50 countries within the Group's geographic coverage.

Data limitations and uncertainty

The carbon footprint data presented in this report may be subject to inherent uncertainty linked to the current state of scientific knowledge and to the quality of external data sources used. Certain figures are sensitive to the methodological choices, assumptions and/or estimates applied in their calculation. Exclusive Networks endeavours to apply best available methodologies and to document its assumptions transparently, while acknowledging that improvements may be made as data quality and scientific knowledge evolve.

Environmental information is subject to review and consolidation procedures designed to support the completeness, consistency and reliability of the information disclosed. This internal control framework draws on certain ESRS principles relating to governance and the reliability of information; it does not imply compliance with the ESRS, nor should it be read as a statement of compliance.

Future Improvements

In line with the Group's commitment to continuous methodological enhancement and improved data quality, several areas for further refinement have been identified for future reporting cycles.

Further work will be undertaken to obtain a more detailed breakdown of energy consumption across operational sites, with the objective of enabling the development of a market-based Scope 2 approach, in alignment with ESRS requirements. In parallel, improvements will be made to enhance the granularity and consistency of waste-related data at site level.

Business travel emissions will be further refined through the full deployment of the Group travel management tool (Navan) in 2026, enabling automated, country-level emissions calculations based on the most up-to-date DEFRA emission factors.

At this stage, greenhouse gas emissions related to purchased cloud computing services and third-party

Environmental Information

data centres are not separately identified or quantified. Consequently, these services are not reported as a distinct sub-category within Scope 3 Category 1 “Upstream purchased goods and services”. This limitation reflects current data availability constraints and will be reassessed in future reporting cycles as data quality and methodological maturity improve.

Finally, future calculations will better differentiate between fully remote and on-site employees, allowing for a more accurate assessment of commuting and workplace-related emissions and better reflecting evolving working practices.

7 Social and societal information

Our people support the Group's growth, operational continuity and ability to respond to changes in the cybersecurity market. The Group's workforce priorities include attracting and retaining relevant skills, supporting employability and career development, promoting employee engagement and wellbeing, and providing an inclusive working environment.

Workforce-related impacts, risks and opportunities are considered through the Group's human resources, risk-management and sustainability processes. A shortage or loss of critical skills may affect operational performance and the Group's ability to deliver its strategy. Conversely, effective workforce development, engagement and responsible employment practices may strengthen organisational resilience and the continuity of expertise.

7.1 Company Workforce

7.1.1 Characteristics of employees

As at 31 December 2025, the Group employed 3,102 people. Unless otherwise stated, workforce indicators in this chapter are reported on a headcount basis and cover employees within the Group's FY2025 consolidation perimeter. Any indicator with a narrower coverage, estimation method or different reference date is identified alongside the relevant table.

The largest regional concentration was in Asia-Pacific (722 employees, 23%), followed by Southern Europe (543 employees, 18%), Central Europe (600 employees, 19%), Northern Europe (694 employees, 22%), META (390 employees, 13%) and the Americas (153 employees, 5%).

Employees by region	2025	%
AMERICAS	153	5%
APAC	722	23%
META	390	13%
NORTH	694	22%
SOUTH	543	18%
CENTRAL	600	19%
Total Group workforce	3102	

The scope of information of employees data is always the 100% of the Group workforce, unless differently specified.

The United Kingdom is the Group's largest country overall with 421 employees, followed by France with 262 employees and Poland with 248.

Compared with 2024, the overall workforce increased by 7%, with growth primarily driven by organic development in core European and Asia-Pacific markets and the integration of acquired entities, in line with the Group's expansion strategy.

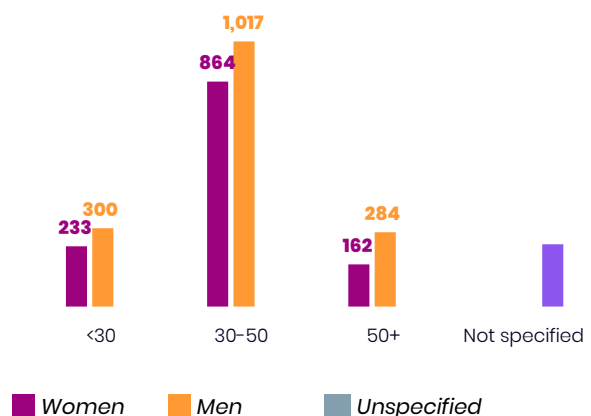
The workforce gender breakdown shows 1,276 women (41%) and 1,622 men (52%), with 204 employees whose gender is not specified (7%). This gender distribution reflects the structural male predominance traditionally observed in the IT and cybersecurity sector. The remaining employees whose gender is not specified represent those who did not identify within a binary category in the Group's HRIS.

By age group, the workforce is structured as follows: employees under 30 total 538 (233 women, 300 men), employees in the 30–50 bracket total 1,889 (864 women, 1,017 men), and employees aged 50+ total 449 (162 women, 284 men). Additional 226 people have not declared their age.

The 30–50 cohort represents approximately 60% of the workforce and constitutes the operational backbone of the organisation.

The relatively stronger representation of women in the under-30 age bracket compared to older cohorts suggests that Diversity & Inclusion policies, combined with generational change in the workforce, are gradually contributing to a rebalancing of gender representation over time, a trend the Group intends to sustain through its ongoing DE&I commitments.

Employees segmentation by gender and age



Of the 3,102 active employees, 242 (7.8%) did not declare the gender and/or date of birth).

Distribution of employees by category and status

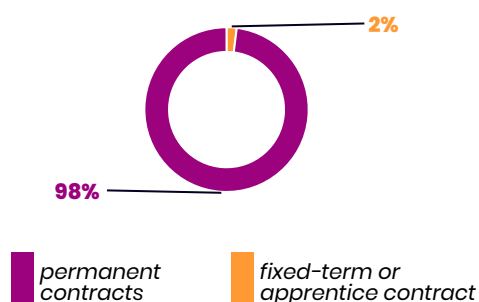
In 2025, the workforce structure remained stable and consistent with previous years. Individual contributors represent 78% of employees and managers 22%, reflecting a balanced organisational structure that supports both operational execution and leadership capacity. Of the managerial population, 26% are women, additional detail on gender distribution across categories is presented in the Diversity & Inclusion chapter..

Employees by category	2022	2023	2024	2025
Individual Contributors	80%	79%	78%	78%
Managers	20%	21%	21%	22%

Employment status is predominantly permanent: 3,040 employees (98%) are engaged under permanent contracts, while 62 employees (2%) are on fixed-term or apprenticeship contracts, comprising 44 temporary employees and 18 apprentices.

The Group continues to favour the use of permanent contracts in order to increase employee loyalty and commitment: (+2% vs last year).

Distribution of employees by status



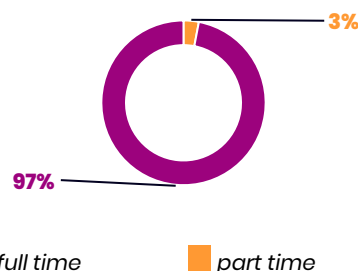
This structure has remained stable over the reporting period and reflects the Group's long-standing approach to fostering employment stability and sustainable workforce development.

Employees by status	2022	2023	2024	2025
Employees on permanent contracts	2,025	2,102	2,788	3,040
Employees on fixed-term or apprentice contract	42	61	107	62

The full-time versus part-time breakdown shows 97% of employees on full-time arrangements and 3% on part-time arrangements. Part-time arrangements are predominantly held by women, who account for 86% of employees under this arrangement compared to 14% men.

This distribution reflects the Group's commitment to flexibility and work-life balance, enabling employees to adapt their working patterns to personal needs while remaining engaged in the organization.

Breakdown of full-time and part-time contracts



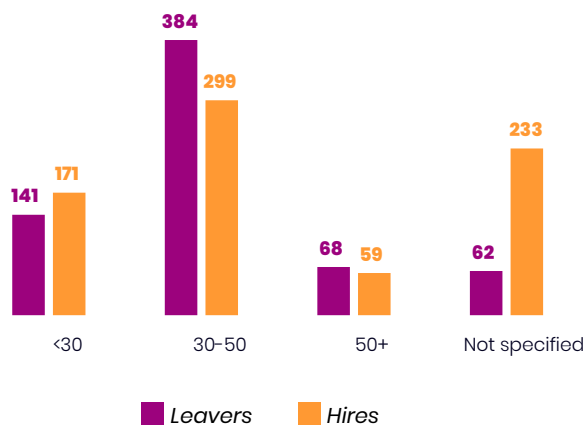
Full-time employees definition : employees whose normal working hours correspond to the standard full-time working time defined under the applicable national laws or collective agreements in the country of employment.

7.1.2 Changes in the number of employees

Total hires in 2025 amounted to 762 employees, while total leavers numbered 655, resulting in a net increase that supported the Group's 7% headcount growth year-on-year. Workforce dynamics by age group are as follows:

- Employees under 30 accounted for 171 hires and 141 leavers, indicating a net positive intake of early-career employees and reflecting the Group's continued investment in young talent.
- The 30–50 age group represented the largest flows with 299 hires and 384 leavers. This cohort's central role in the Group's operations means it drives both the highest volume of recruitment activity and the highest absolute number of departures.
- Employees aged 50+ saw 59 hires against 68 leavers, consistent with natural career progression and retirement patterns at this stage.
- Not-specified age accounted for 233 hires and 62 leavers, reflecting the addition of employees whose age data was not captured at the time of reporting, primarily linked to newly integrated entities.

Hires and leavers by generation in 2025



As is common in the digital, cybersecurity and broader technology sectors, the Group also relies on a number of external consultants who contribute across several regions, notably in finance and information technology functions. These individuals, referred to as "non-employees" under ESRS, provide specific expertise but are not part of the Group's salaried workforce and are therefore excluded from the employee figures disclosed in this performance statement in accordance with CSRD requirements.

In 2025, overall departure levels is to those observed in 2024, which were also higher than historical averages due to the privatization of the Group, its delisting, and related organizational changes. While still elevated, turnover trends are gradually moving back toward more normalized levels.

	2024	2025
Employees turnover	13.90 %	21.50 %

Turnover is total leavers during the year / average headcount per month of the year. It includes permanent, fixed terms and apprentices

The split between voluntary and involuntary departures remained broadly stable compared to 2024, with voluntary departures accounting for approximately 64% of total exits, mainly driven by career development and professional ambitions, and involuntary departures representing approximately 36%, primarily attributable to structural changes associated with the ongoing organisational transformation.

Termination category



■ Voluntary leavers

■ Involuntary leavers

7.2 Governance of social issues

The Human Resources Department, is dedicated to «anticipating and securing the future of Exclusive Networks by attracting, developing, and retaining top talents. Its mission is to shape the organization of tomorrow by implementing effective structures and processes that enhance company performance and ensure long-term sustainability. Led by the Chief People Officer, the department plays a strategic role within the company. As a member of the Executive Committee, she works closely with the Chief Executive Officer, maintaining regular communication to align HR initiatives with the company's overall vision and objectives».

The Human Resources Department operates at two levels:

- at the head office level: the teams at the head office bring together the expertise of Tools, Data and Programmes, Compensation and Benefits, Recruitment and Skills Development, and aim to support and equip the HR operational teams in a homogeneous way; and
- at the Local/Regional level: the regional operational Human Resources Business partners, attached to the Country Managers, are responsible for implementing global programmes and supporting operational activities.

This organisational structure thus makes it possible to preserve the agility, specificities and uniqueness of the countries.

The Chief People Officer oversees the company's HR policy, working closely with both Field and Corporate HRBPs and specialized HR teams at headquarters, including the HR Development, Recruitment, and Compensation & Benefits departments, as well as the Tools Data and Analytics.

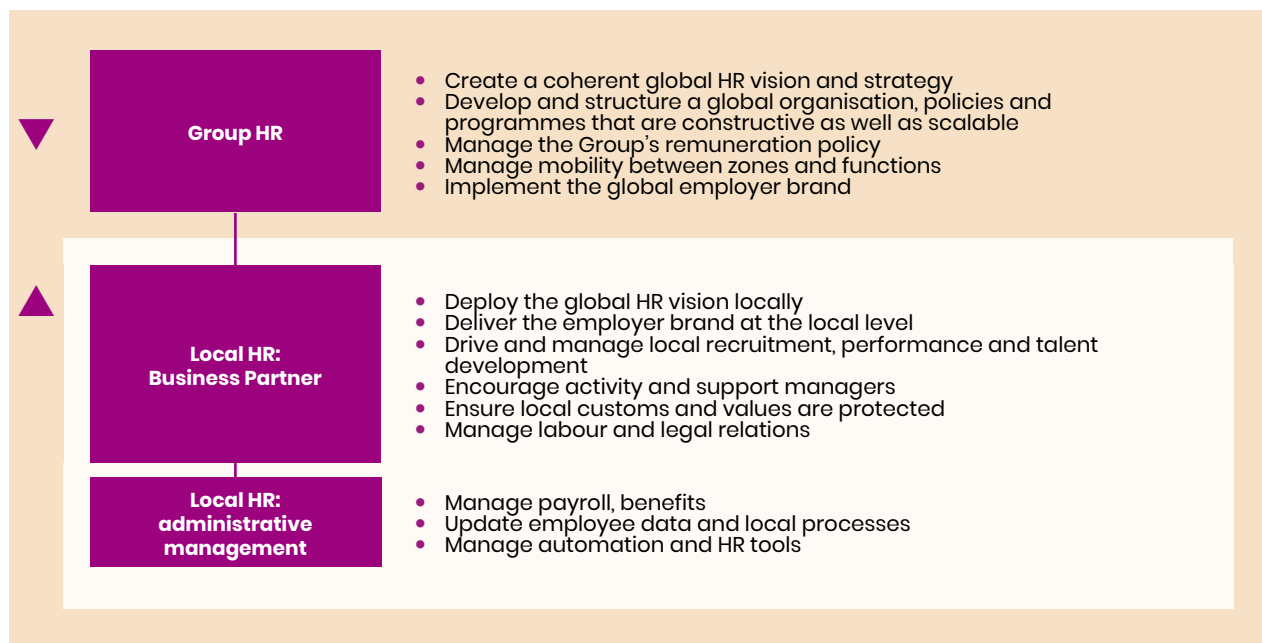
To ensure strategic alignment, weekly meetings are held with all HR directors to define key priorities, such as recruitment, retention, compensation, development, and diversity & inclusion—and to monitor the successful implementation of initiatives at the local level.

The Executive Committee is responsible for approving diversity, equity, and inclusion (DE&I) goals and initiatives. Based on its recommendations, the Board of Directors sets objectives for gender diversity in managerial roles.

Review and validation of the implementation of the social strategy

The Chief People Officer reports on social performance and initiatives at the Group level, regularly presenting the results to the Executive Committee for review. These outcomes are also shared with the Board of Directors at least once a year.

If certain targets are not met, the underlying reasons and corrective actions are discussed during Board meetings. Additionally, the Chief People Officer leads efforts to promote diversity, equity, and equal opportunities, ensuring these initiatives are presented to the same governance bodies.



Roll-out

The human resources strategy is deployed in collaboration with the regional human resources teams in order to be adapted to local specificities and challenges.

Since 2021, in order to support the Group's strong international growth and equip itself with reliable and consistent people data, the Human Resources function has progressively deployed a global Human Resources Information System (HRIS), ensuring harmonised management, monitoring and continuous improvement of HR processes across the Group.

This system enables:

- the centralisation and real-time updating information
- the improvement and standardization of processes as well as the monitoring of employee career paths from recruitment to departure; and
- the automation and increased reliability of leave management, performance reviews, career development and compensation processes
- automation and making leave requests, performance reviews, career development and remuneration processes more reliable.

Since the summer of 2025, the Group has further strengthened its digital HR ecosystem through the deployment of Workday as its global Human Capital Management platform. This transition represents an important milestone in the Group's HR transformation journey, providing enhanced data quality, increased process harmonisation and improved visibility across the employee lifecycle. Workday supports more integrated talent, performance and workforce management processes, while enabling greater responsiveness to business needs and organisational changes.

This global HR infrastructure enables real-time analysis of workforce trends, including headcount evolution, employee turnover and other key workforce indicators. Continuous monitoring is supported through configurable dashboards and reporting tools, including Power BI, facilitating data-driven decision making at both local and Group levels. The HRIS also interfaces with other specialised applications, including employee engagement survey platforms, interview management tools and self-service solutions that provide employees with secure access to their administrative documents and HR information.

In addition, the Human Resources function has reinforced its analytical capabilities through the introduction of dedicated People Analytics expertise within the HR team. This capability enhances the quality of workforce analysis, strengthens forecasting and workforce planning, and provides deeper insights to support strategic business decisions. By leveraging data and predictive indicators, the HR function is increasingly able to anticipate organisational needs, identify trends and support sustainable growth through informed and evidence-based decision making.

Through these investments in systems, data governance and analytical capabilities, Human Resources teams continue to improve efficiency, reliability and forward-looking workforce management. The availability of robust and timely information allows for objective decision making, greater anticipation of future challenges and a stronger focus on high value-added activities that support both employees and the long-term development of the Group.

7.3 Social Dialogue and Engagement

Employees are central to the Group's performance and long-term success. Exclusive Networks considers social dialogue and employee engagement to be key drivers of satisfaction, talent retention, and the preservation of critical expertise, all of which directly support business performance. Ensuring employee commitment and well-being is therefore a core responsibility of the Group.

In a highly competitive labour market, particularly in the cybersecurity sector, where skilled talent remains scarce, the Group closely monitors the risk of employee attrition and deploys targeted retention measures.

Excessive turnover, especially in key roles, could constrain growth, making employee retention a strategic priority.

Policy and engagement

Exclusive Networks promotes close, day-to-day interaction between management and operational teams to ensure employees are heard and can openly express concerns.

This approach to social dialogue and internal communication was further strengthened in 2024 with the arrival of a Global Communications Director.

In 2024, the Group set a target of reaching a 77% engagement rate by 2025. Engagement stood at 66% in 2025, and this target was not met, reflecting the impact of significant structural changes following the Group's privatisation and delisting, including a period of organisational uncertainty that affected employee sentiment. As the Group's social strategy is currently under review as part of the broader 2024-2030 strategic update, the engagement target will be reassessed and a revised trajectory published in due course. This rate is measured by aggregating several questions relating to pride in belonging to the Group, recommending the Group as an employer, motivation to work for the Group, and projecting oneself in the Company for more than two years.

Key monitoring indicators	2022	2023	2024	2025
Percentage of employees responding to the annual employee feedback survey on the total of employees	80 %	84 %	78 %	79 %
Engagement rate	72 %	71 %	69 %	66 %
Percentage of employees covered by collective agreements across the Group *	N/A	18,9%	17%	17%
Percentage of employees covered by collective agreements across Economic European Area (EEA) only **				37%

* Collective bargaining coverage (%) = (Number of employees covered by collective bargaining agreements ÷ Total number of employees) × 100

** Workers' representative coverage in EEA countries with significant employment (more than 50 employees) is calculated by dividing the number of employees covered by a representative body by the total headcount in the relevant countries. On this basis, workers' representatives cover 34% of employees across the applicable EEA countries.

Employee survey participation has remained consistently high over the period, stabilising at 79% in 2025, which reflects sustained employee willingness to engage and provide feedback despite ongoing organisational changes. The engagement rate shows a gradual decline from 72% in 2022 to 66% in 2025, mainly reflecting the impact of significant structural transformations, including the delisting and associated changes.

With regard to collective bargaining coverage, the proportion of employees covered by collective agreements at Group level remains structurally lower, at around 17% in 2024–2025. This should be considered in the context of the Group's global footprint and local labour frameworks, as coverage within the Economic European Area (EEA) alone reaches approximately 37%. These differences primarily reflect national regulatory environments rather than limitations in social dialogue practices.

Actions implemented

Internal Surveys

Since 2021, Exclusive Networks has conducted its annual internal satisfaction survey, "Your Voice Matters", open to all employees worldwide and led by the Human Resources Department with the support of the Group Chief Executive Officer.

The survey enables employees to share their experience and perceptions across key themes, including engagement and pride in belonging, quality of management, work-life balance, collaboration and communication, effectiveness at work, recognition, and training and personal development.

In 2025, the survey recorded:

- a 79% Group participation rate, remaining stable compared to 2024 (78%), which confirms sustained employee involvement despite ongoing organizational changes.
- The engagement rate reached 66%, down from 69% in 2024 and 72% in 2022, reflecting the impact of structural transformations following the Group's delisting rather than a decline in employee commitment.
- Satisfaction survey participation has remained consistently high over recent years, demonstrating a resilient culture of dialogue and continuous improvement.

Key strengths identified in 2025 include:

- strong relationships with direct managers,

- employees' perception that their work is meaningful and contributes directly to Group performance,
- clear roles and responsibilities.

At the same time, the survey underscores the need for continued progress in systems and processes, leadership communication and employee engagement, innovation, and reward and recognition. These dimensions remain critical enablers of employee engagement and play an important role in attracting, retaining and developing talent while supporting the Group's long-term performance and growth ambitions.

The Group's objective is to continue an annual monitoring of employee engagement in order to be as close as possible to their expectations and concerns.

In addition, since 2020, when leaving the Company, each employee can participate in a survey during which they will be able to express the reasons for their decision, share information about their experience within Exclusive Networks and their future professional prospects. This measure makes it possible to identify new practices that are likely to meet employees' expectations.

Institutional social dialogue

The Exclusive Networks group strives to establish a constant and high-quality social dialogue, in compliance with the legislation in force in each country where it operates, as well as in countries where it is not subject to a legal obligation. Social relations are placed in each country under the authority of the Country Manager and the Human Resources Manager, who are responsible for:

- setting up all legal bodies in accordance with local legislation; and
- facilitating regular meetings and dialogue with staff representatives and social partners, where they exist.

In 2025, 17% of employees were covered by collective bargaining agreements at Group level, a proportion that reflects the Group's global footprint and the heterogeneity of national labour frameworks across the countries in which it operates. Coverage is significantly higher within the European Economic Area (around 37%), where collective agreements are more widespread due to established regulatory frameworks and stronger social dialogue traditions.

In countries like Austria, Belgium, Italy, Portugal and Spain the rates are confirming at the 100%.

In France, 91% of employees were represented through the Social and Economic Committee (CSE) as of 31 December 2025. Employee representative bodies were regularly informed and consulted on key organisational developments, transformation initiatives and projects that may impact employees, including organisational changes and restructuring initiatives. Discussions also included information shared through the BDESE platform, the presentation of the Gender Equality Index, the CSE's annual accounts, and remuneration-related agreements, including profit-sharing arrangements and related payments.

Local agreements on working conditions and/or employee remuneration are also in force across a number of the Group's subsidiaries.

Categories	Country	Nature of the agreement
Agreements with an impact on compensation	France	Participation Agreement Profit-sharing agreement
Agreements that have an impact on working conditions	France	Agreement on flat-rate pay in days over the year
	UK	Agreement on remote working

Other channels of social dialogue

In addition to these bodies, the Group's Code of Conduct sets out the main principles applicable to all employees who have the opportunity to raise their concerns through the whistleblowing procedure.

7.4 Ensuring fair and attractive remuneration and benefits

Context

In a context of high competition in the global labour market, especially in the cybersecurity sector where there are not enough qualified employees, it is essential that the Group ensure the competitiveness of remuneration levels, which are rising. This is an important lever for attracting and retaining talent.

A higher turnover, particularly in key positions, could ultimately penalise the Group's growth.

Policy

The Group's policy is to offer everyone a fair and competitive remuneration in the market that reflects the performance and levels of responsibility associated with each person's roles. To this end, the Group aims to position itself at the level of benchmark best practices observed in comparable sectors. This initiative takes into account local laws and business practices in each region. Thus, the skills and level of responsibility associated with the roles of

employees are compensated by a fixed salary in line with the experience acquired and the practices observed for each profession on the market. Employees are also remunerated by variable remuneration schemes (bonus or commission), depending on the level of responsibility and the country.

Most enabling, corporate, and management functions participate in bonus plans that combine collective and individual performance objectives. In contrast, employees with direct responsibility for revenue generation, sales performance, or billable services participate in commission plans, where commissions represent a significant proportion of their variable compensation.

The remuneration policy includes performance incentive plans that must meet the objectives of mobilising key employees towards medium- and long-term performance by encouraging outperformance, associating these employees with the Company's valuation and building loyalty.

Key monitoring indicators

	2022	2023	2024	2025
Share of employees with a performance-related variable component in their remuneration	88%	90%	91%	96%

Adequate wages

The Group is committed to providing remuneration that meets or exceeds applicable statutory minimum wage requirements in each country in which it operates. In addition, the Group assesses pay levels against external market benchmarks using data from Willis Towers Watson (WTW) and Mercer Comptrix.

Compliance with these requirements is reviewed annually through the Group's compensation review process. Based on the methodology applied and the scope of the assessment conducted during the reporting period, the Group considers employee pay levels to be aligned with its commitment to providing adequate wages.

Actions implemented & systems

Since its IPO (Initial public offering) in 2021, the Exclusive Networks group aims to associate and align the financial interests of management and a number of key contributors (Group executives, executive committee members, senior executives, talent and experts) with those of shareholders, including through long-term incentive plans (LTIPs). This additional remuneration mechanism aims to motivate and retain beneficiaries by directly involving them in the Group's development.

As a result, a limited number of employees (senior managers, talents and experts) were allocated performance shares in order to link them to the Company's long-term performance and financial results. The definitive acquisition of the allocated shares is subject to the fulfilment of performance conditions and a condition of presence in the Group on the vesting date. The performance indicators used are based on the Group's financial performance.

While no new LTIP have been granted since 2025, previously awarded performance share plans remain outstanding and continue to vest in accordance with their original terms and conditions.

Collective agreements with an impact on employees' remuneration

Collective performance remuneration schemes may exist in some countries, whether they are mandatory legal schemes (profit-sharing in France, for example) or voluntarily set up by the Group according to local practices, such as profit-sharing in France, these schemes, where they exist, are accessible to all employees.

As of FY2025, 17% of the Group's total global workforce is covered by a collective bargaining agreement with an impact on compensation, compared with 19% in FY2024 the year-on-year change reflects headcount growth concentrated outside jurisdictions with established bargaining frameworks (notably APAC and AMER) rather than a reduction in coverage within any single geography.

Within the European Economic Area, coverage is substantially higher, at 37% of employees, reflecting more established regulatory frameworks and social dialogue traditions in the region; several EEA countries (including Austria, Belgium, Italy, Portugal, and Spain) report coverage at or near 100%. The Group will continue to refine and disaggregate this indicator in future reporting cycles.

Remuneration and development

The 2025 annual payroll, including salaries and payroll taxes, extracted from the consolidated financial statements of the Exclusive Networks group, was €255 million, up 11% year-on-year. This increase is linked to, among other things, the increase in the number of employees, the impact of exchange rates, the increase in salaries and the effect resulted from recently acquired entities.

Overall, more than 95% of the Group's workforce has performance-related compensation components.

7.5 Career and Skills Development

7.5.1 Attracting – Identifying – Retaining Talent

Exclusive Networks operates in a fast-evolving cybersecurity ecosystem where technological innovation, business transformation and regulatory developments continuously reshape skills needs. The Group therefore considers career development and skills enhancement as key enablers of long-term performance, employee engagement and business resilience. Investing in people supports Exclusive Networks' ability to anticipate market changes, deliver value to partners and customers, and foster sustainable growth across its international footprint.

Career and skills development is embedded in the Group's sustainability strategy for 2024–2030, which recognises human capital as a critical driver of value creation alongside operational excellence, responsible partnerships and the development of the broader cybersecurity ecosystem. By supporting employees' employability, professional growth and internal mobility, Exclusive Networks seeks to mitigate talent-related risks, strengthen retention and ensure continuity of expertise in a highly competitive labour market.

Governance and policies

The Group's approach to career and skills development is underpinned by human resources policies applicable across its operations and aligned with applicable labour standards and international frameworks. These policies promote equal access to training and career opportunities, non-discrimination in professional development, and lifelong learning for all employees.

Responsibilities for implementing and monitoring career and skills development initiatives are shared between Group-level functions and local management teams, ensuring both strategic consistency and adaptation to local contexts. This governance framework forms part of the broader due diligence processes relating to the own workforce, as required under ESRS, and supports the identification and management of material impacts, risks and opportunities linked to skills, employability and workforce transformation.

Actions implemented

Increase the Group's visibility and employer brand

Exclusive Networks is committed to strengthening the visibility of its employer brand and its presence on all recruitment channels. To achieve this, the communication and human resources teams work closely together to promote the company on various social networks, particularly LinkedIn, as well as platforms favored by younger generations as part of its strategy to attract top talent.

Regularly published articles, videos, and photos showcase the company, strengthen its employer brand, and highlight job opportunities. Exclusive Networks shares job openings on its website, LinkedIn, and Indeed, along with local platforms such as Jobstreet or Glassdoor, Kununu (in Germany), Pracuj (in Poland), Magment (in Dubai), etc.

Referral policy (Co-option)

In order to attract quality candidates, the Group has implemented internal referral programs that empower employees to promote job openings and recommend qualified candidates from their network. Employees who successfully refer a candidate who is hired are rewarded for their contribution.

Internal mobility

The attractiveness of Exclusive Networks is closely linked to its ability to support employees' professional development and long-term career progression. Internal

mobility, in all its forms—functional, geographical, lateral and vertical—enables employees to deepen their expertise and strengthen their understanding of the Group's services, business lines and strategic priorities, while offering attractive and ambitious career pathways.

In 2025, Exclusive Networks officially launched a **Group-wide Internal Mobility Policy** designed to support employee development, enhance talent retention and optimise internal skills deployment. Internal mobility is a key component of the Group's people development strategy and allows employees to apply for open positions across teams, functions and geographies through a transparent, fair and consistent process aligned with business needs.

The **internal mobility programme** is open to all permanent employees who meet defined eligibility criteria and ensures equal treatment between internal and external candidates. Opportunities are managed through a structured recruitment process, with clearly defined roles and responsibilities for employees, managers and HR. The programme is governed by standardized procedures, local legal compliance requirements and non-discrimination principles, contributing to workforce engagement, operational continuity and long-term talent planning.

Academic Relations

With a view to strengthening its reputation and constantly enriching its pool of candidates, the Group maintains privileged relationships with the best training courses (universities and schools) for all its professions, and in particular, with the academies in the field of cybersecurity training the cybersecurity engineers and salespeople of tomorrow. In addition, internships and apprenticeship contracts are offered to students in order to train them and prepare them for recruitment following their graduation.

The CyberFarm Academy at California Polytechnic State University San Luis Obispo

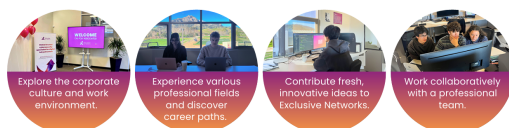
Exclusive Networks addresses the structural cybersecurity skills gap through CyberFarm, a dedicated talent development program based at California Polytechnic State University, San Luis Obispo. The initiative is designed to strengthen employability, inclusion, and long-term resilience across the cybersecurity ecosystem while contributing to the Group's broader CyberESG ambition to create shared value with partners and vendors.

Launched within Exclusive Networks North America, CyberFarm provides students with hands-on, learn-by-doing experience in a real corporate environment, enabling them to bridge the gap between

academic learning and the practical skills required by the cybersecurity industry. The program operates in close collaboration with Exclusive Networks' technology vendors, who actively oversee and guide students' day-to-day activities, ensuring strong alignment with industry needs and expectations.

Participants are engaged as associate resources for a one-year program, combining academic commitments with weekly working hours structured to fit university schedules. Students are embedded in operational teams and work directly with vendors and channel partners across multiple functions, including sales, marketing, finance, technical and engineering roles. This exposure allows participants to develop practical, job-ready skills while contributing meaningfully to ongoing business operations.

Associates Are Able To:



Exclusive Networks provides a true corporate office environment on campus, including all necessary infrastructure, systems and tools, ensuring students operate under professional conditions comparable to those of a standard business setting.

In addition, the Group supplies comprehensive HR services, covering recruitment, onboarding, training, coaching and ongoing support, with a dedicated on-staff HR Business Partner assigned to the program. Functional management support is also provided as needed, including sales, marketing, technical and engineering oversight.

CyberFarm supports a smoother transition into professional cybersecurity careers, with a significant proportion of participants progressing into employment opportunities, often with partner vendors, following completion of the program.

By improving access to real-world cybersecurity roles, the initiative directly responds to the sector-wide shortage of skilled talent while strengthening the long-term availability of critical capabilities required to secure digital infrastructures.

The program currently engages approximately 20–30 students per year and continues to expand as partnerships and offerings grow. A key milestone was recently reached with the onboarding of the 100th CyberFarm participant, reflecting the program's scalability and growing impact.

By investing in early-career talent, fostering practical skill development and strengthening diverse talent pipelines, CyberFarm contributes to positive social outcomes while reinforcing Exclusive Networks' role in advancing an inclusive and resilient cybersecurity ecosystem. This initiative illustrates how the Group integrates social considerations into its business model, aligning talent development with ecosystem-wide transformation and sustainable growth.

Key monitoring indicators

Number of associates integrated into the Cyberfarm program	20–30
--	-------

Percentage of graduates hired in the cyber channel ecosystem after completing the program	85%
---	-----

Weekly hours of training and work at vendors'	15–20
---	-------

The global talent identification program : *RiseUp*

The human capital management policy includes an annual process that aims to identify the Company's key employees and developing succession plans covering major and high-responsibility positions.

The objective is to identify potential successors for these roles within varying timeframes, ensuring their development and readiness while also identifying positions where internal succession is lacking or unavailable.

To support this, the Group's Human Resources Department has continued and expanded its global talent identification and retention initiative, the *RiseUp* Programme.

This programme aims to identify, recognise and develop a certain number of talents across the Group, covering different functions, technical or leadership skills, and thus build a talent pool that will be one of the key success factors for the Group to achieve the set objectives.

With the support of local Human Resources managers, country managers, and team leaders, the program annually identifies a select group of high-value employees. Their performance and potential for growth and career advancement are then carefully assessed. Once identified, each person receives a personalized development plan tailored to their needs. Implemented at both the local and Group levels, the plan combines group-wide initiatives with individualized components and includes mentorship. Additionally, raising a talent community helps strengthen team spirit, reinforce connections with the company, and build a strong internal talent network.

This process ensures that high-potential individuals are clearly identified, recognised and supported as part of an enriching development path, to achieve their full professional potential and bring their expertise to the Group.

Succession Plan

The Exclusive Networks group establishes a succession plan for a number of strategic functions, at a global and local level, thus anticipating the departure of a key employee performing an essential function requiring experience and whose replacement would be difficult, and to ensure the continuity of the organisation and the achievement of the Company's objectives.

This succession plan is built in several phases:

- identification of key functions - management positions, unique, specific and instrumental positions requiring highly specialised skills essential to the Group's development;
- identification of employees likely to move towards these positions in the short, medium or long term with

the support of Human Resources managers and line managers; and

- implementation of specific measures and actions to support the development of identified employees' skills.

This succession plan is closely linked to the *RiseUp* programme and is now part of an annual event. The Human Resources Department is also attentive to diversity in all its forms of the people identified in succession plans, whether in terms of gender, profile or nationality.

Key monitoring indicators		2022	2023	2024	2025
Talent Identification & Retention	Number of employees integrated into the <i>RiseUp</i> programme	35	31	15	31
	Percentage of employee retention integrated into the <i>RiseUp</i> programme	83 %	100 %	94 %	88 %

This process of identifying key positions is shared with the Executive Committee.

7.5.2 Developing employees' skills Context

Policy

Exclusive Networks supports and is committed to promoting the development of its employees' skills, in particular through internal and external training or e-learning, which is essential for the transmission of knowledge and know-how and thus gives employees the opportunity to continue to learn and evolve. In addition, internal mobility offers are available to employees to enable them to enrich and diversify their professional experience.

Several action plans (collective and individual) have been implemented by the Group in order to support, encourage and guide the development of its employees' skills and to promote team performance:

- performance appraisal and career development processes in which employees share their desire for development and training with their managers;
- collective and individual training and development policies;
- internal mobility policies;
- succession plans (see above).

Training & Individual Development

The Group offers a broad range of comprehensive training programmes designed to enable employees to continuously develop and strengthen their skills. These programmes cover a wide variety of themes, including managerial and leadership development, as well as professional effectiveness.

Training formats are tailored to the subject matter, target audience and learning objectives, and may be delivered in person or remotely through e-learning modules and virtual classes, either in group settings or on an individual basis.

Employees have access to three main types of training.

- Technical training aims to maintain and further develop employees' professional and technical expertise, which is particularly critical in the cybersecurity sector, where innovation and technological change are constant. This includes, but is not limited to, training and certification programmes provided by technology partners and suppliers on new products or solutions, which in some cases are required for employees working on these technologies.
- Soft-skills trainings focus on the development of behavioural, interpersonal and personal capabilities, supporting collaboration, leadership, adaptability and long-term performance across the organisation.
- In addition, the Group deploys a broad set of mandatory training courses covering policies, risk management, compliance and cybersecurity. These courses are periodically updated or repeated to ensure consistent coverage and awareness across the workforce.

As part of its sustainability strategy, Exclusive Networks has also developed a dedicated ESG and cybersecurity training module, CyberESG, which aims to raise awareness of the interconnections between cybersecurity and sustainability, reinforcing employees' understanding of their role in supporting long-term value creation.

Key monitoring indicators	2022	2023	2024	2025
Number of available training sessions	228	971 (completed courses)	60	145
Number of employees who have taken at least one course	524	477	2895	3102

Actions implemented

Performance Appraisal & Career Development

An annual performance appraisal process is in place to enable all employees to discuss with their manager their performance over the past year, objectives for the year ahead, work-life balance, training and development needs, and longer-term career development prospects. This process applies to the 100% of Group employees present in the company as of 30 September of the previous year.

The appraisal is conducted in two phases.

- The first phase consists of a self-assessment, launched in January, which allows employees to reflect on their achievements, assess how they have delivered results, and evaluate how they perform their role in practice, including identifying strengths and development areas. This stage also provides an opportunity for employees to review how they organise their work and to consider their work-life balance.
- The second phase takes place in early February and consists of a formal review meeting with the manager. This discussion enables a shared assessment of performance, alignment on objectives, identification of development and training priorities, and dialogue on career progression, thereby supporting individual development and long-term talent management within the Group.

Employee perceptions of managerial feedback are monitored through the annual engagement survey. In this context, 79% of respondents agreed with the statement “My manager gives me useful feedback on how well I am performing”, highlighting the role of regular feedback in supporting engagement and performance.

7.5.3 Building Cybersecurity Skills Across the Ecosystem

A secure and resilient digital economy depends on people as much as technology. As part of our pillar “Advancing the Cybersecurity Ecosystem”, Exclusive Networks invests in the development of cybersecurity skills across its value chain, helping partners, customers, end users and future professionals build the expertise required to meet evolving cyber threats. This commitment directly supports our sustainability ambition by strengthening digital resilience, enhancing employability, and helping close the global cybersecurity skills gap.

In 2025, Exclusive Networks and its training business, including Consigas, trained 13,627 learners through a broad portfolio of cybersecurity courses and certification programmes. Training was delivered to a diverse audience including channel partners, enterprise customers, end users and individual professionals seeking to advance their cybersecurity capabilities. Courses covered a wide range of technologies, with a particular focus on Palo Alto Networks and Fortinet solutions, while also providing training across numerous other leading cybersecurity vendors. According to the Exclusive Training Services catalogue, the portfolio includes technical, security, cloud, networking and emerging technology courses offered through authorized training centres and specialist training providers.

To maximize accessibility, training is delivered through multiple formats, including instructor-led classroom sessions, on-site programmes and virtual learning environments. While in-person training remains available for practical and collaborative learning experiences, the majority of courses are now delivered virtually, enabling learners across geographies to access high-quality cybersecurity education. Exclusive Networks’ training centres support both technical and sales-oriented cybersecurity learning and provide customized training pathways tailored to customer and partner needs.

Professional certification remains a key component of the learning journey. In 2025, learners could access leading vendor-accredited certifications, including the Palo Alto Networks Accredited Certification pathway and the Fortinet Network Security Expert (NSE) programme. Available certifications ranged from professional and specialist qualifications to advanced architect and expert-level credentials, enabling cybersecurity practitioners to continuously develop their expertise and demonstrate industry-recognized skills. Fortinet training alone included 13 courses with an average course duration of 2.84 days and certification opportunities covering NSE 4 through NSE 8 levels.

Across all programmes, the average training duration reached 23.7 hours per learner, reflecting the technical depth required to build practical cybersecurity capabilities and maintain expertise in a rapidly evolving threat landscape.

7.6 Human and Labour Rights commitments

Context

Respect for human rights is fundamental to responsible business conduct. As a global distributor operating across five continents, Exclusive Networks recognises that its responsibility extends beyond its own workforce to its business relationships and value chain. The Group promotes a culture of respect for people and is committed to upholding internationally recognised human rights in all countries in which it operates.

Policy

In view of the Group's rapid growth in recent years, its international development and its presence on five continents, and the expectations of its stakeholders on this major issue, in 2023 the Group finalised the implementation of major policies relating to the respect of human rights. This work involved governance as well as all employees. The human rights commitments enshrined in the Code of Business Conduct and Human Rights Policy include:

- respect for fundamental human rights, as described in the Universal Declaration of Human Rights adopted by the United Nations General Assembly on 10 December 1948, and in the International Labour Organization's Declaration on Fundamental Principles and Rights at Work adopted in 1998 and amended in 2022;
- Decent working conditions, through the organisation and resources required to protect employee health and safety, comply with applicable labour laws and social regulations in every country of operation, particularly regarding working hours, rest periods and holidays, and ensure fair remuneration commensurate with qualifications and skills;
- Equal opportunities, through policies and procedures that prohibit and remedy any form of discrimination,

both at the point of hiring and throughout employment, and that actively promote diversity and inclusion as a source of strength for the Company;

- Skills development, enabling employees to continue learning and building the capabilities that underpin the Group's performance in the cybersecurity sector;
- Respect and dignity in all dealings with and between employees.

Salient geographies

The Group's operations are predominantly located in geographies assessed as presenting a low risk of human rights violations. This assessment is based on Freedom House country scores, with territories scoring above 50/100 classified as "free". On this basis, 88% of the Group's permanent workforce is employed in low-risk geographies.

The Group's human rights commitments also extend to consumers and end-users and are aligned with internationally recognised frameworks, including the **UN Guiding Principles** on Business and Human Rights. In practice, these commitments are given effect through ethical business conduct, data protection and the responsible use of the Group's solutions. Monitoring and compliance are supported by a whistleblowing channel open to all stakeholders, internal and external, enabling concerns or potential adverse human rights impacts to be reported. The Code of Conduct, which incorporates these expectations, is shared with partners during onboarding and is publicly available, supporting awareness and accountability across the value chain. Together, these mechanisms also provide access to remedy where adverse human rights impacts are identified.

Key monitoring indicators

		2023	2024	2025
Respect for human and labour rights	Share of permanent employees in countries without human rights risk	79%	86%	88%

Actions implemented

Channels to raise concerns and access to remedy

Since 2021 the Group has operated an externally managed whistleblowing system, accessible to employees and to external stakeholders including partners and end-users, allowing the reporting of any conduct contrary to the Code of Conduct. Reports are handled confidentially under the supervision of the Group Ethics Officer.

The Group applies a strict prohibition of retaliation against any person raising a concern in good faith. Where a violation is confirmed, it is investigated and an associated action plan is implemented. The existence and accessibility of the channel is communicated through the Code of Conduct, which is publicly available and shared with partners at onboarding.

Commitments to the prevention of psychological harassment

Exclusive Networks prohibits any conduct that may offend the dignity of individuals, in particular any form of harassment. Situations of this nature are addressed through the whistleblowing procedure described above.

Awareness and communication

Exclusive Networks prohibits any conduct that may offend the dignity of individuals, in particular any form of harassment. Situations of this nature are addressed through the whistleblowing procedure described above.

Organisation of working conditions

Working time is organised according to the Group's operational needs and within the framework of local regulations, which vary between jurisdictions. The Group is committed to complying with applicable rules on working hours, rest periods and holidays across all its sites. Working conditions and social dialogue are addressed in more detail in the preceding sections.

The Group must constantly develop its sites in order to improve its operational performance and the working conditions of its employees.

7.7 Diversity, Equity and Inclusion (DE&I)

Context

The Group promotes a diverse, equitable and inclusive world free from bias, gender stereotypes and discrimination and where difference is valued and celebrated. Diversity, equity and inclusion are the daily reality of how we live and work within the Exclusive Networks group, and how we work with all business partners.

Diversity, equity and inclusion are fully integrated into the Company's organisation in all areas and at all stages of working life: recruitment, training, compensation, geographical mobility and career development.

The Group is convinced that its performance depends on the quality and commitment of its employees and that a pleasant and respectful working environment benefits everyone and makes the Group more efficient and productive. Respect for individuals and equal opportunities are core values of Exclusive Networks. All employees, managers and executives must take part for the strategy to be effective. Executives are the guarantors of this for all their employees.

Promoting this environment is an important lever for attracting, creating loyalty and retaining talent, ensuring their engagement and fostering and creating places and spaces where all employees thrive. It is by building on these values that the Group will continue to deliver superior business results, sustainable growth and drive innovation to maintain its competitive edge in its industry.

Policy

Exclusive Networks wanted to strengthen its commitment to diversity and inclusion with the launch of its first diversity, equity and inclusion policy on 8 March 2023, International Women's Day. In particular, the Group undertakes to:

- create an inclusive work environment;
- promote equal opportunities and combat all forms of discrimination;
- promote diversity and equality of resources in all their forms: creation of action plans focussed on career advancement, equal pay, training and work-life balance;
- promote cultural and ethnic diversity, and diversity of origins: Exclusive Networks expects its employees to recognise, respect, and welcome all cultural differences wherever it operates;
- respect and accept all sexual orientations and gender identities; and
- take into account intergenerational differences: it is important for Exclusive Networks to value both the

experienced vision of seniors and the innovative spirit of young talent.

This policy, as well as the Code of Conduct, which sets out the commitments in terms of non-discrimination, formalise the commitments to mutual respect and diversity within the Group.

As part of this policy, Exclusive Networks is committed to fostering, adopting, encouraging and preserving a culture of diversity, equity and inclusion (DE&I) and to taking concrete actions to combat all forms of discrimination.

This policy supports and aims to contribute to the achievement of the United Nations Sustainable Development Goals, in particular Goal 5. The Group is committed to implementing a more sustainable way of working and living by respecting all employees, regardless of their origin, gender, sexual orientation, political point of view, religious belief, social status or any other personal condition.

As part of its DE&I journey, the Group is focussing its efforts on four major issues, which are associated with an action plan, performance indicators and a timetable for implementation:

- **ensure the representation of women in management positions** (members of the Executive Committee and their N-Is, Regional Managers, Country Managers and their Management Committees among countries with a turnover of more than €100 million);
- **improve employee awareness and understanding of diversity**, inclusion and equity through training modules;
- **promote equal access to opportunities** for all employees through a single, transparent access and process on the career page of the Company's website; and
- **ensure equal treatment** of men and women.

Despite the actions taken, the ability to recruit women in the field of engineering and cybersecurity remains constrained by their under-representation in educational courses and careers related to computer and digital technologies. Nevertheless, the distribution of men and women within the Company, which can be constantly improved, appears to be very positive.

Exclusive Networks may need to evolve its processes and objectives in response to progress on these topics, or to take into account new business needs and objectives.

A progress report is presented each year to the Board of Directors, covering the initiatives implemented as well as the progress of the various objectives.

Key monitoring indicators		2023	2024	2025
	Number and proportion of women in managerial positions*	38%	32%	29/113 26%
	Number and proportion of women in C-suite positions (definition by ILPA diversity template) **			2/4 50%
Awareness and Understanding of DE&I	Percentage of employees that have approved the Diversity and Inclusion policy	67%	63%	79.0%
	Proportion of women participating in the <i>RiseUp</i> global talent acceleration programme	45%	44%	35%
Equal treatment of men and women	Gender Equality Index (out of 100) ***	97/100 EXN SAS 98/100 Everest SubBidCo	96/100 EXN SAS 74/100 Everest SubBidCo	92/100 EXN SAS 55/100 Everest SubBidCo

* Calculated on the people who identified themselves in a binary gender (male or female)

** ILPA definition of C-suite position : the Chief Executive Officer and any senior executives reporting directly to the CEO (e.g. CFO, COO, CAO).

*** The Gender Equality Index is calculated in accordance with the methodology prescribed by French regulations. As part of this methodology, pay gap calculations are based on age groups rather than position level or individual responsibilities. Furthermore, the relatively small size of the employee population (fewer than 100 employees) may increase year-on-year variability and limit the statistical smoothing typically observed in larger populations. The index is calculated each year for the previous year. Only the two French entities, EXN SAS (Exclusive Networks, Simplified Joint Stock Company) and Everest SubBidCo, are subject to the Gender Equality Index (IEFH), a regulatory indicator for French companies with more than 50 employees.

Actions implemented

Ensuring the representation of women in leadership roles

The Group conducted a study on the share of women in various management positions and proposed an action plan to the Executive Committee and countries to help accelerate the transformations underway. Various actions have been undertaken, in particular:

- specific monitoring of women in talent review: the annual performance review system makes it possible to identify professional development or mobility projects for employees, in particular, projects developed by women, including those aspiring to become managers. Among our employees, a selection of the 31 most promising talents, 35% of whom are women, participate in the *RiseUp* training program to promote access to positions of responsibility. The 24-month *RiseUp* programme contributes to the development of inclusive leadership skills in future managers. Since the program's launch, our Top Talents group has averaged 41% women, illustrating Exclusive Networks' commitment to gender equality within its leadership in the present and future years.
- particular attention is also paid to female profiles as part of the process of identifying key collaborators and drawing up the succession plan.
- the Group has put in place an inclusive hiring process and ensures that shortlists for management positions include women, and actions are taken as part of the recruitment process to ensure that employees include female profiles, whether they are candidates or employees involved in the selection process for future talent.

Awareness and understanding of Diversity, Equity and Inclusion

In order to support the DE&I policy, raise employee awareness of the issues associated with it, and prevent any risk of discrimination, the Group developed two online training modules in 2023:

- the first module, "Diversity and Inclusion", provided employees with an overview of the importance of diversity and inclusion in their daily interactions and decision-making processes with the aim of enabling them to better understand how to foster an environment that values differences;
- the second module, "Unconscious Bias" allowed employees to explore this concept and its potential impact on their interactions and perceptions. By acknowledging and addressing these biases, Exclusive Networks is able to ensure fair and impartial treatment of all employees to enable them to better understand the issues, increase their knowledge of these topics, and fight against all forms of discrimination.

This training is carried out by local human resources teams, available in all countries, and is accessible to all employees. In 2024, this training will be an integral part of the mandatory training integrated into the onboarding of new employees.

Non-discrimination in all its forms is an integral part of recruitment and management training modules. Managers are thus made aware of professional equality between men and women.

Equal treatment of men and women – Pay equity

In addition to actions to promote equal treatment of men and women in recruitment and access to training (see above), the Group strives to offer attractive and fair remuneration that contributes to employee loyalty and the Group's performance. Remuneration policies are based on the principles of non-discrimination and equity between employees regardless of gender, and are structured through an evaluation based on required skills and shared objectives assessed against objective criteria.

The Group measures the gender pay gap in two ways:

- based on a career salary index (men/women index) whose calculation and publication methods are regulated; the index stands at 92/100 for Exclusive Networks (France) and 55/100 for Everest SubBidCo by 2025; The Gender Equality Index is calculated in accordance with the methodology prescribed by French regulations. As part of this methodology, pay gap calculations are based on age groups rather than position level or individual responsibilities. Furthermore, the relatively small size of the employee population (fewer than 100 employees) may increase year-on-year variability and limit the statistical smoothing typically observed in larger populations
- the difference between women's average total pay compared to men's average total pay by job level. The calculation is based on the employees' full compensation, including base salary, target variable compensation, and other benefits. The number of employees taken into account includes permanent employees, regardless of their contract, and excludes trainees and apprentices (for reasons of relevance, when there are less than five male or female employees per level, the calculation is not made).

7.8 Health and Safety

Context

Exclusive Networks' commitments are aimed at providing all employees with working conditions that ensure their health and safety in compliance with laws and regulations.

The nature of the Group's activities as well as the small number of employees per company explains why very few of them are certified according to a health and safety standard, without reflecting the importance of this subject for the Group and the commitment of Human Resources Managers as close as possible to the local teams. As a result, 10% of the workforce is represented in a collective health or safety proceeding and 8% are employed in a company with health or safety certification.

Work-life balance is also an important driver of employee engagement and retention.

Policy

In terms of health and safety, the Group focusses its actions mainly on the mental health of its employees, more specifically, the reduction of stress at work.

Exclusive Networks also endeavours to ensure that its practices in terms of the organisation of work and other time spent in the Company aim as far as possible to maintain a good work-life balance, in particular allowing for the proper exercise of parenthood. This topic is an ongoing focus that echoes the pressure to which the entire cybersecurity sector is subject due to the skills shortage. The internal survey, which is carried out every year, measures the level of satisfaction of employees with regard to work-life balance, and 82% satisfaction rate of employees stating that they are confident that their manager cares about their own wellbeing.

The Group has put in place a global policy on hybrid work based on everyone's trust and responsibility. It encourages ways of organising work to improve the quality of life at work while reducing travel time.

Key monitoring indicators		2022	2023	2024	2025
	Number of fatalities as result of work-related injuries and work-related ill health of other workers working on undertaking's sites				0
	Number of recordable work-related accidents for own workforce				0
	Number of days lost to work-related injuries and fatalities from work-related accidents, work-related ill health and fatalities from ill health related to employees				365*
Work-life balance	Number of employees on permanent contracts working part-time	124	125	107	105

*The days lost are related to an accident happened the year before.

Actions implemented

Reducing stress at work

As part of its general risk prevention policy, Exclusive Networks is committed to promoting a quality environment for its employees, which reduces psychosocial risks. Through the annual satisfaction survey, Exclusive Networks measures employees' appreciation of their working conditions and thus detects situations that generate difficulties at work.

The major initiative launched in 2023 to better take into account stress at work and the potential need for support and guidance, particularly of a psychological nature, has been the implementation of an Employee Assistance Programme (EAP) in all our countries.

Since 2023, numerous local initiatives have emerged, exploring the integration of animals in the workplace. Recognized for their positive effects on well-being, these initiatives have been linked to stress reduction, relaxation, improved concentration, and enhanced interactions among colleagues.

In the United Kingdom, trials were conducted in 2023, incorporating employees' pets and even llamas into the workplace.

In the UK, Belgium and the Netherlands, free lunches were also introduced to reduce any financial stress.

In addition, a whistleblowing procedure has been introduced and cyberbullying is taken into account.

Hybrid work

Finding a balance between on-site and remote work is essential to ensure work-life balance.

The Group always allows employees to work from home as much as possible while preserving time in the office in order to maintain collaboration and strengthen the sense of belonging and teamwork. To this end, in addition to local collective agreements on working conditions, the Group has implemented a global hybrid work policy since 2021, intended to serve as a guide for management and employees alike.

This policy determines the Exclusive Networks group's philosophy on flexible working and is implemented and adapted at the local level, to take into account the applicable regulations and the specificities of each company. It can be formalised via teleworking or flexible working agreements in certain geographies where the Group is present, such as the United Kingdom.

This policy gives the possibility to agree to fixed and/or occasional teleworking days, thus allowing up to two teleworking days per week.

In 2024, this policy covered all countries in which Exclusive Networks is present with local adaptation where necessary.

In addition to enabling a better work-life balance, this policy also helps to limit the travel time and environmental impact of employees' commuting.

As part of the annual performance evaluation of employees, workload is taken into account in setting goals in order to reconcile professional and personal life, among other things, via the annual satisfaction survey.

Arrangement of working time

In addition to this hybrid way of working, Exclusive Networks ensures that requests for flexible working time, such as requests for part-time work as well as statutory or personal leave made by employees in compliance with applicable laws and regulations and when activities allow it.

7.9 Consumers and end-users

Policy

The rapid increase in cyber threats targeting businesses, public institutions and critical infrastructures represents a major risk in an increasingly digitised and dematerialised global environment. As a global leader in the distribution of cybersecurity products and services, Exclusive Networks contributes to reducing malicious cyber-attacks, thereby supporting the protection of data, critical infrastructures, healthcare systems, governments and companies worldwide.

To address these challenges, the Group has established a robust governance framework and organisational structure designed to prevent, detect and respond effectively to cyber threats. Information security and cyber resilience are embedded into the Group's operating model and are considered essential to safeguarding customers, partners and end-users across the value chain.

In 2025, Exclusive Networks further strengthened its cyber resilience by applying recognised information security and risk management methodologies, aligned with the ISO 27000 family of standards and other leading international frameworks. The Group's information security risk management practices are aligned with ISO/IEC 27005:2022 (Information Security Risk Management), which complements and reinforces the principles set out in ISO/IEC 27001.

This commitment was formally confirmed in 2025 with the achievement of **ISO/IEC 27001 certification**, attesting to the effectiveness, maturity and continuous improvement of the 100% of the Group's Information Security Management System (ISMS).

This certification demonstrates Exclusive Networks' ability to manage information security risks in a systematic, documented and auditable manner, in line with international best practice.

7.9.1 Governance and organisation of information systems security

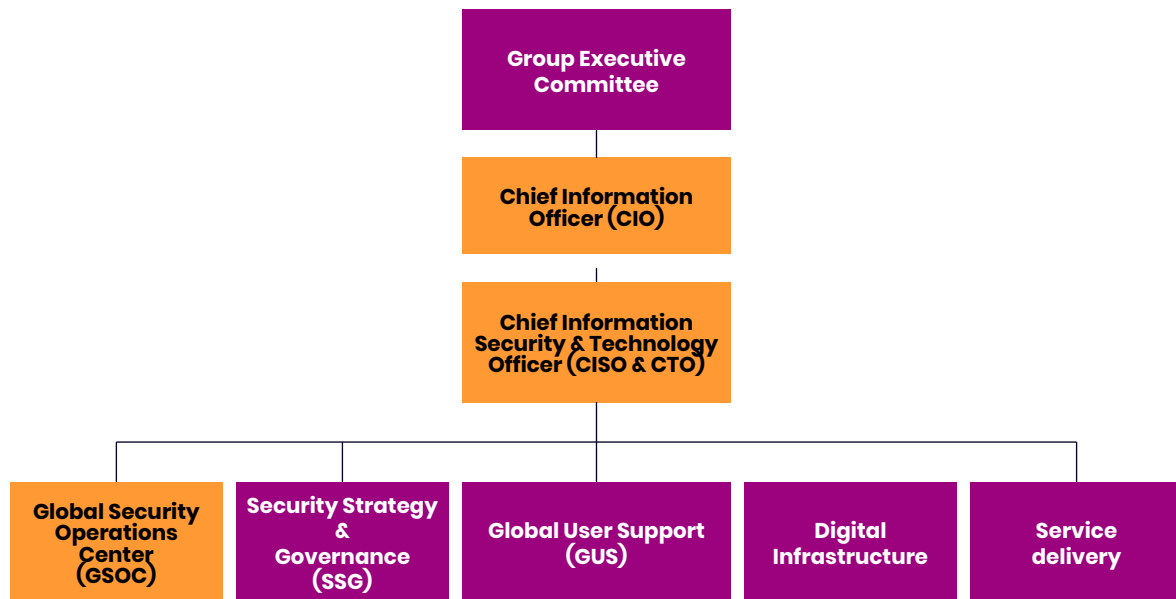
The Information Systems Security function relies on a centralised and multidisciplinary organisation, placed under the authority of the Chief Information Security Officer & Chief Technology Officer (CISO & CTO). This organisation brings together dedicated information systems security officers and specialised teams responsible for protecting the Group's information assets and digital operations.

Key components of this governance framework include:

- The Global Security Operations Centre (GSOC), which is responsible for managing security incidents across the Group, covering both local infrastructures and offices worldwide.
- The GSOC is supported by an external Managed Endpoint Detection & Response (EDR) service, providing 24/7 monitoring and response capabilities and the ability to initiate legal investigations where necessary.
- The Security Strategy & Governance (SSG) team, established in 2023, which is responsible for developing and implementing the Group's operational model for IT security governance. This includes oversight of the ISMS, AI governance, information risk management, device and data security strategies, access management, and security awareness initiatives.

Together, these functions contribute to securing the Group's information systems and ensuring the confidentiality, integrity and availability of information exchanges with customers, suppliers and, more broadly, Exclusive Networks' partners. Through this governance framework, the Group supports the protection of consumers and end-users by strengthening trust, resilience and security across the cybersecurity ecosystem.

Organisation of the security of Information Systems



component elements of the Cyberdefense council

The Exclusive Networks' information security governance is led by the Chief Information Security Officer and Chief Technology Officer (CISO & CTO), who holds full authority over the security infrastructure of the Group across all geographies. The combination of CISO and CTO responsibilities in a single role ensures efficient deployment of security policy and proximity between IT and security teams.

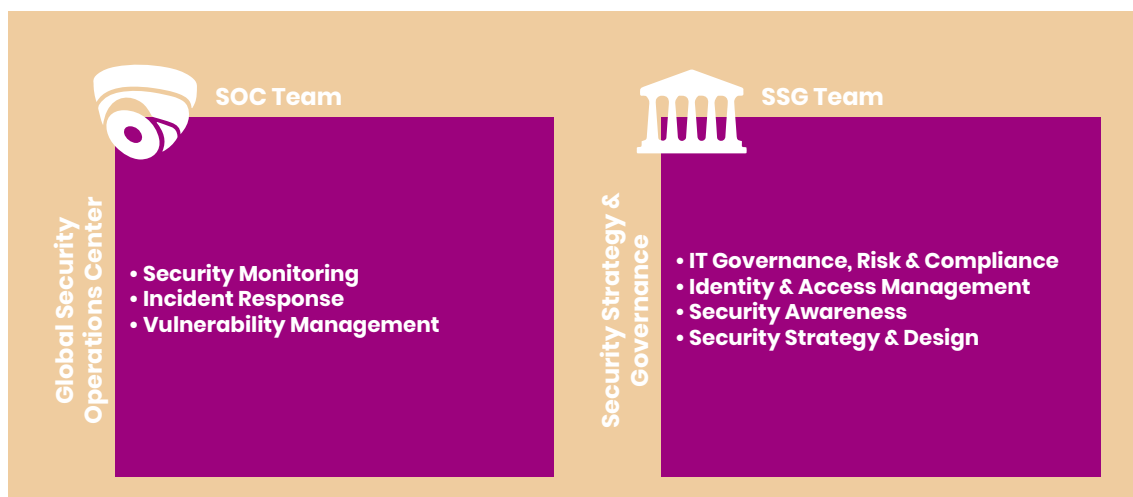
The CISO & CTO reports directly to the Chief Information Officer, a member of the Group's Executive Committee.

The governance structure is supported by two dedicated teams:

- The Global Security Operations Centre (GSOC) – responsible for security monitoring, incident response and vulnerability management across all Group entities, supported by an external Managed Endpoint Detection & Response service operating 24/7.
- The Security Strategy & Governance (SSG) team – responsible for IT governance, risk and compliance, identity and access management, security awareness, and security strategy and design.

The Digital Infrastructure and Workplace teams, previously reporting to the CTO, have been consolidated under the leadership of the CISO, strengthening cross-functional collaboration and cybersecurity resilience across the organisation.

Security Teams & Responsibilities



External security and public scoring

Exclusive Networks actively monitors and publicly demonstrates its cybersecurity posture through industry-recognised exposure scoring platforms, including RiskRecon and SecurityScorecard. These tools provide transparent, externally visible assessments of the Group's security exposure, accessible to partners and the broader market.

Maintaining strong scores on these platforms is not only a matter of internal risk management, but certain strategic partners also require a minimum score as a prerequisite for business engagement, making security posture a direct commercial consideration. In 2025, the Group undertook targeted remediation efforts, including the decommissioning of unused websites and demo lab environments, resulting in significant improvements to its public security scores.

Certification of the Global Security Operations Center

The Group's Global Security Operations Centre was officially certified at the end of 2023 by Trusted Introducer, the European Computer Emergency Response Team (CERT) service that lists, accredits, and certifies security teams according to verified maturity levels. Certification is assessed against the Security Incident Management Maturity Model (SIM3), which evaluates four areas of action: Organisation, Human, Tools and Procedures.

7.9.2 Information System Protection

In 2023, the Group rolled out its Information Security Risk Management procedure, aligned with the ISO/IEC 27005:2022 standard. This procedure defines how the Group identifies, prioritises, manages and monitors risks concerning its information assets, operations and projects, ensuring the confidentiality, integrity and availability of the Group's systems, information and services.

Already since 2024, the Group has been operating under a new Information Security Management System (ISMS), aligned with ISO 27001. An internal audit was completed in 2024 to validate the compliance of processes and documentation ahead of formal ISO 27001 certification, achieved in 2025.

Deployment

In order to carry out its mission, the following security tools have been deployed and implemented in a centralised, standardised, and automated manner:

1. Asset management: asset lifecycles, asset and software inventory;
2. Data capture and behavioural analysis of users and entities (Security Information and Event Management and User and Entity Behavioural Analysis), using artificial intelligence;

3. Email security;
4. Managed Endpoint Detection & Response using artificial intelligence and behavioural analytics;
5. Vulnerability management;
6. Endpoint and patch management;
7. Identity and Access Management, using artificial intelligence and behavioural analytics;
8. Web security (Cloud Access Security Broker and Secure Access Service Edge) using artificial intelligence and behavioural analytics;
9. Security Orchestration Automation and Response (SOAR);
10. Threat Intelligence: An instance of the Malware Information Sharing Platform (MISP) that identifies, analyses, and shares cyber threat intelligence with other organisations.

The majority of the selected vendors and solutions come from the Exclusive Networks portfolio of cybersecurity products and solutions, and are recognised as a "Magic Quadrant Leaders" by Gartner (a leading technology assessment consulting firm).

Cyber Exposure Score (CES)

The Cyber Exposure Score (CES) measures the Group's relative cyber risk by assessing its exposure to threats and the criticality of its assets, including workstations and servers. Maintaining a "Low" CES level, defined as below 350, is a key monitoring indicator supported by regular patching, system updates and proactive vulnerability remediation.

In the final quarter of 2025, Exclusive Networks maintained a low CES for the third consecutive year since 2022, demonstrating the tangible benefits of close collaboration between infrastructure and security teams.

Reporting

The Group has expanded the security information provided to the Executive Committee and Country Managers. This communication is based on regular security communication and reporting. This includes information on the latest security threats and trends, reporting via KPIs on the Group's cyber exposure as well as statistics on security alerts, attack simulation results and more.

Exclusive Networks achieved its target of maintaining an average Cyber Exposure Score of "Low" or below ahead of schedule in 2024, maintained this level in 2025, and continues to monitor the indicator annually to manage fluctuations in the evolving cyber-threat landscape.

Key monitoring indicators		2022	2023	2024	2025
Control and follow-up of IT security incidents	Number of incidents reported through the reporting set up by the Group	2,254	2,846	2,336	929
Monitoring and controlling the level of risk in terms of exposure to threats	Average Cyber Exposure Score (CES)*	384	333	329	334

* Indicator subject to a 2025 target

Thanks to the actions carried out by the various Global IT teams, Exclusive Networks managed to achieve an ATL (All Time Low) for CES in the last quarter of 2024. The overall trend for 2024 is downward, illustrating the added value of cooperation between infrastructure and security teams.

Actions implemented

- Information Security Management System (ISMS):** Implementation of our ISO 27001-aligned ISMS to ensure a holistic approach to information security across the organization. An internal audit was carried out in 2024 to validate the compliance of our processes and documentation for ISO certification in 2025.
- Cybersecurity Training:** Updated security awareness program to improve employee training at Exclusive Networks. Developments include targeted training, simulation exercises and dedicated sessions during Cybersecurity Month.
- Threat Intelligence:** Strengthening the use of threat intelligence in our Security Operations Center (SOC) to improve our monitoring and analysis of emerging cyber threats.
- IT Service Continuity & Disaster Recovery:** Development of a continuity and disaster recovery plan to ensure the availability of IT services supporting critical business processes.
- Collaboration:** Participation in sectoral cybersecurity initiatives and cooperation with partners to share threat information and best practices.

Trainings carried out during the year 2025

	Q1	Q2	Q3	Q4
General awareness training				
Tailored awareness training		●		
Cybersecurity awareness month				●
Bites & Bytes	●	●	●	●
Security alerts & News				
Quarterly security newsletter	●	●	●	●
Phishing simulations	●	●	●	●

Tool implementation for phishing

Phishing remains one of the most pervasive and rapidly evolving cybersecurity threats globally, targeting employees, partners and end-users through increasingly sophisticated social engineering techniques. In 2025, the widespread use of generative artificial intelligence further amplified the scale, credibility and automation of phishing campaigns, increasing the potential for data breaches, financial losses, service disruption and reputational damage.

Social and societal information

To address this risk, Exclusive Networks implemented phishing simulation and monitoring tools to track key behavioural indicators, including the phishing email clicking rate and the reporting rate of suspected phishing attempts.

Monitoring these indicators enables the Group to identify trends, target awareness actions more effectively and reinforce a culture of vigilance and ethical conduct, in line with ESRS G1 expectations on risk prevention and responsible business conduct.

Key monitoring indicators		2022	2023	2024	2025
Employee training and awareness of IT security	Number of training modules provided to all Group employees	7	10	11	15
	Email sent				+
	Average clicking rate*				6.38%
Phishing Simulation	Average reporting rate*				24.17%
	Number of incidents reported via the Group's reporting system**	2,254	2,846	2,336	929
	Cyber Exposure Score (CES)*	384	333	329	334

*CES is the annual average of a continuous flow of data over the year.
**Incidents are aggregated monthly based on data collected from the various security tools in place.

7.9.3 Data protection

Context

Protecting personal data is crucial for maintaining employees', partners' and customers' trust and complying with data privacy regulations.

Companies must implement appropriate measures to ensure the confidentiality, integrity, and availability of personal data.

Data protection is an essential component of responsible business practices and ethical data management.

Exclusive Networks Approach

Exclusive Networks is committed to protecting the personal data of its customers, partners, and employees. The company recognizes the importance of data privacy and complies with all applicable data protection regulations, including the General Data Protection Regulation (GDPR).

Key pillars of the data protection policy

1. Data Minimization: Collecting and processing only the personal data that is necessary for legitimate business purposes.
2. Data Security: Implementing appropriate technical and organizational measures to protect personal data from unauthorized access, use, disclosure, alteration, or destruction.

3. Rights of data subjects: Respect the rights of data subjects, including the right to access, rectify, erase and restrict the processing of their personal data.
4. Transparency: Provide transparent information to data subjects on how their personal data is collected, used and protected.
5. Accountability: Commitment to ensure the protection of personal data and to comply with applicable regulations.

Key actions implemented

1. Data Protection Impact Assessments (DPIAs): Conducting DPIAs to assess and mitigate privacy risks associated with new projects and initiatives.
2. Data Breach Response Plan: Developing a data breach response plan to effectively manage and respond to data breaches.
3. Notification of Breaches to regulatory authorities: Reporting data breaches to the relevant local data protection offices when required by law
4. Privacy by design: Integrate privacy considerations into the design and development of new products and services.
5. Employee Training: Provide data protection training to employees to raise awareness and ensure compliance.

7.9.4 IT Governance & Information Security

Context

1. Cybersecurity is essential to protect businesses and consumers in an increasingly digital world.
2. Companies must put in place robust cybersecurity measures to protect sensitive data and maintain the trust of their customers and partners.
3. Strong cybersecurity governance and organization are essential for effective risk management and appropriate incident response.

Exclusive Networks Approach

Exclusive Networks recognizes the importance of cybersecurity for both its own operations and those of its customers and partners. The company is committed to implementing robust cyber security measures to protect sensitive data and maintain the confidence of its stakeholders.

Key pillars of the data protection policy

1. **Risk Management:** Implementing a comprehensive risk management approach to identify, assess, and mitigate cybersecurity threats.
2. **Incident Response:** Establishing a robust incident response plan to effectively manage and recover from cybersecurity incidents
3. **Security Awareness:** Educating employees and stakeholders about cybersecurity threats and best practices to promote a security-conscious culture
4. **Technology and Innovation:** Leveraging advanced technologies and innovative solutions to enhance cybersecurity capabilities.
5. **Collaboration:** Collaborating with industry partners and sharing threat intelligence to strengthen collective cybersecurity defences.
2. **Cybersecurity Training:** We updated our security awareness program to improve education Exclusive Networks employees receive. Changes include targeted trainings, tabletop exercises and cyber security month sessions and more.
3. **Threat Intelligence:** Increased utilization of threat intelligence in our Security Operations Center (SOC) to improve our security monitoring and insights in emerging cyber threats.
4. **IT Service Continuity & Disaster Recovery:** Establishing a formal continuity and disaster recovery plan to ensure availability and of IT services that support critical business processes.
5. **Collaboration:** Participating in industry cybersecurity initiatives and collaborating with partners to share threat intelligence and best practices.

Key actions implemented

1. **Information Security Management System (ISMS):** Operationalization of our ISMS aligned with ISO 27001 standard to ensure a holistic approach for information security covering the 100% of the Exclusive Networks Group. We performed an internal audit in 2024 to validate the compliance of our processes and documentation in preparation for ISO certification in 2025.

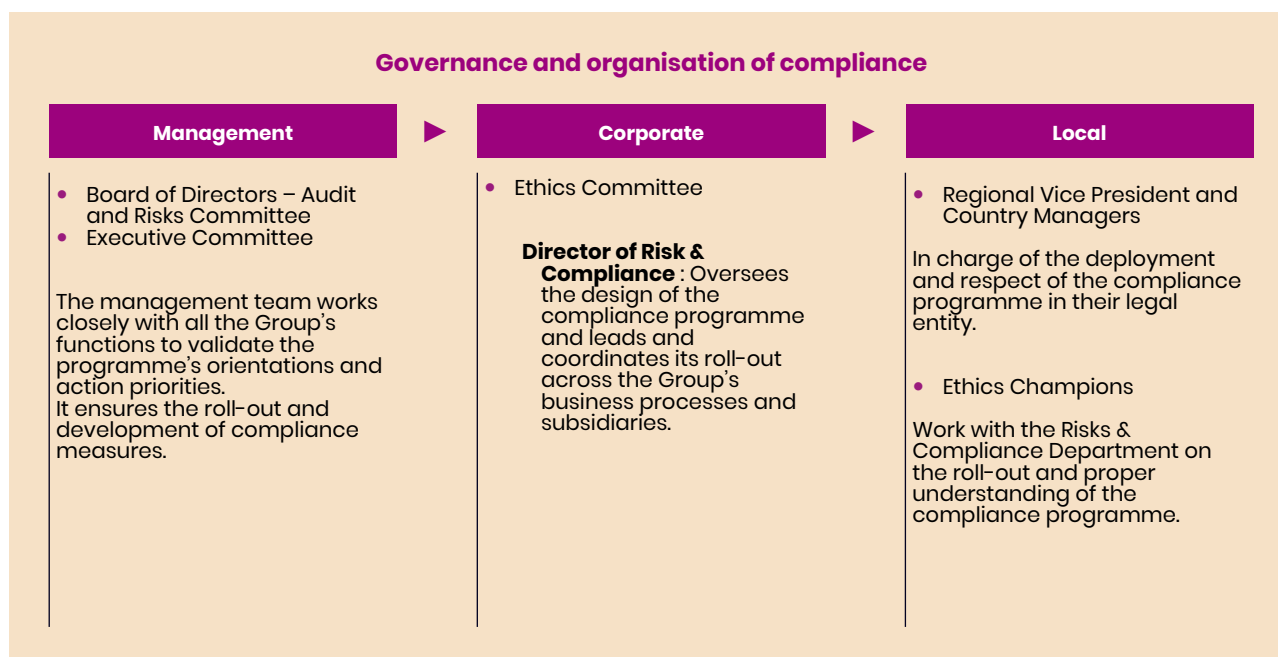
8 Corporate culture and business conduct policies

8.1 Compliance governance and organisation

Exclusive Networks is committed to conducting its activities with integrity, transparency and accountability. The Group's approach to business conduct and compliance is designed to prevent unethical behaviour, mitigate governance-related risks and promote

responsible business practices across its operations and value chain. This governance framework supports long-term value creation and reinforces trust with stakeholders.

To deploy and manage the compliance programme, the Group relies on a dedicated organisation described below:



At the management level

Board of Directors – Audit and Risks Committee, provides independent oversight of the Group's anti-corruption and compliance framework, reviews key compliance risks, monitors significant investigations and remediation plans, and receives regular updates on compliance programme effectiveness.

Executive Committee, sets the tone from the top, promotes a culture of ethics and integrity, and ensures that compliance objectives and anti-corruption initiatives are effectively embedded across the Group's operations. The Executive Committee oversees the implementation of the Ethics & Compliance Programme, supports the allocation of appropriate resources, reviews key compliance developments and investigations, and ensures that compliance considerations are integrated into strategic and operational decision-making.

At the corporate level

The Group's General Counsel and Chief Compliance Officer, who reports to the Chief Financial Officer, is responsible for overseeing the Group's Ethics & Compliance framework and ensuring its effective implementation across the organisation. The role includes defining the compliance strategy, supervising the compliance function, and regularly reporting on compliance matters to the Executive Committee, the Audit & Risk Committee and the Board of Directors. It shall decide freely, and independently, on any internal investigation it deems appropriate and which shall be entrusted to internal audit.

Ethics Committee, is chaired by the Group Chief Legal & Compliance Officer and comprises the Chief Executive Officer, Chief Financial Officer, Chief Revenue Officer, Chief People Officer and the Director of Risk & Compliance. The Committee provides strategic oversight of the Group's Ethics & Compliance Programme, reviews key compliance risks, significant investigations, whistleblowing matters and remediation initiatives, and monitors the effectiveness of the Group's ethics and compliance framework. It also promotes accountability and reinforces ethical leadership across the organisation.

The risk and Compliance Director

The Director of Risk & Compliance reports to the Group Chief Legal & Compliance Officer and is responsible for the design, implementation and continuous improvement of the Group's Ethics & Compliance Programme, including its anti-corruption framework. The role oversees compliance risk assessments, compliance monitoring activities, policy management, training and awareness programmes, regulatory monitoring and the coordination of the Group-wide compliance network. The Director of Risk & Compliance serves as the primary point of contact for operational functions on compliance matters and supports internal investigations, remediation actions and whistleblowing processes where required.

At the local level

Regional Risk and Compliance Managers are appointed by the Director of Risk and Compliance and report directly to him/her. They are responsible for deploying and maintaining the compliance programme within their respective regions, ensuring alignment with Group policies, applicable laws and local regulatory frameworks. Their responsibilities include, in particular:

- drafting and updating local procedures and internal controls;
- maintaining an effective control environment within their region;
- raising employee awareness and delivering compliance-related training;
- reviewing and validating high-risk third parties; and
- managing internal investigations related to compliance matters.

Country Managers are responsible for the deployment and effective application of the compliance programme within the legal entities under their responsibility. They ensure that local operations comply with Group policies and applicable regulations and that compliance requirements are embedded into day-to-day business activities. Country Managers are also responsible for reporting locally identified risks and significant compliance issues to the Executive Committee and/or the Director of Risk and Compliance, thereby supporting effective governance and decision-making at Group level.

Regional Vice President, are accountable for driving compliance ownership within their regions, overseeing the effective implementation of Group policies, challenging local management when necessary, and promoting a strong culture of ethics and integrity.

The Ethics Champions Network

The network of Ethics Champions, with around 50 employees, has as its main mission to implement the compliance program in conjunction with the Risk and Compliance department, and to ensure that it is properly taken into account and understood.

They are the Risk and Compliance Department's relay points in local entities and the point of contact for all questions relating to the compliance program.

A quarterly call point between the Ethics Champion and the Risk and Compliance Manager in his region to review the deployment of key elements of the compliance program in his entity, and more specifically:

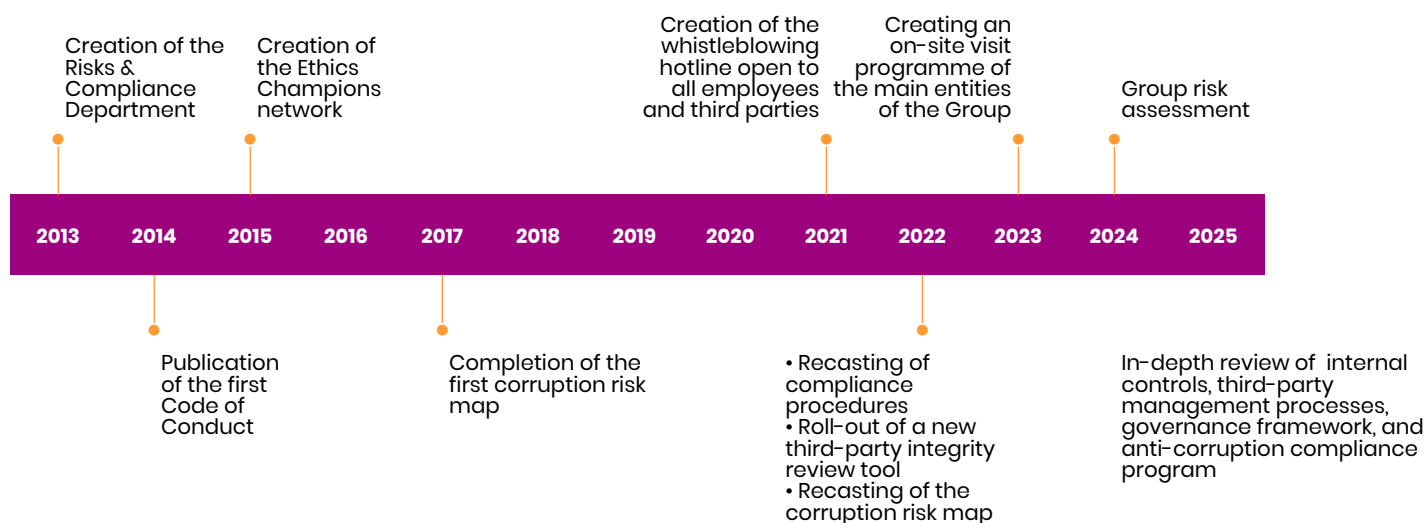
- Gift and invitation declarations recorded in the internal tool;
- The signature rate of procedures, in particular the Code of Conduct;
- Communications issued by the Ethics Champion and the Country Director;
- Completion of compliance training and participation rate;
- Tracking of third parties integrated in the integrity review platform;
- Follow-up to the action plan for corruption risk mapping.

8.2 Ethics, prevention and the fight against corruption

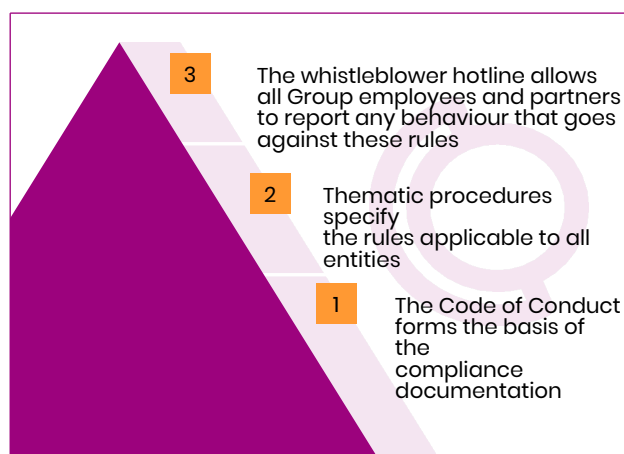
A mature compliance programme

Adopting and promoting honest and ethical behaviour in all its relations and with all its partners is a strong commitment of the Exclusive Networks group. This principle has led the Group to define rules of conduct in terms of ethics, intended for its employees as well as for all its business partners and stakeholders.

Key date in the Group's compliance policy



Through its internal policies and procedures, the Group establishes the guiding principles applicable to all its subsidiary companies, designed to provide employees with the rules of good conduct and behaviour to adopt in terms of business ethics and the fight against corruption. The compliance programme is structured as follows:



- Training of employees and more specifically the key function and exposed function to ensure clear role and responsibility
- Improved level 2 controls, including on-site visits and in-depth reviews by regional managers
- Corruption risk assessment : In 2025, the Group launched a comprehensive refresh of its anti-corruption risk assessment to reassess corruption risks across all regions, functions and key business activities. The project aims to identify emerging risks, evaluate the effectiveness of existing mitigation measures, and further strengthen the Group's anti-corruption framework in line with regulatory expectations and business developments

The Exclusive Networks Group's corruption prevention program includes policies and procedures such as the Code of Conduct, the Conflict of Interest Policy, or the Gifts and Invitations Policy. All procedures and policies are addressed individually to each employee as soon as they are hired through the Group's e-learning platform. They give rise to an acknowledgment of receipt as well as a questionnaire to ensure that they are properly understood.

In order to robustly address the risk of corruption or non-compliance with internal business ethics regulations and procedures, the Exclusive Networks group regularly updates and develops its compliance programme, to take into account its corruption risk map as well as new regulatory and legal requirements.

In 2025, the Group continued to update and complete its corruption risk management system on three major measures:

- Updating the third-party onboarding system and monitoring its deployment;

Follow-up of the site visit program and strengthening level controls

In 2023, the Risk and Compliance Department launched a new "Onsite Visit" entity visit program to ensure the effective deployment of the anti-corruption program at local level.

The program of visits includes:

- Face-to-face training for all employees. The topics covered are intended to strengthen the understanding and awareness of risks within the organization;
- Targeted interviews with key functions such as the Country Manager, HR, Marketing, Sales, Finance and Ethics Champion to deepen understanding of the specific risks in each area;
- The monitoring of the implementation of the programme, which involves in-depth discussions and testing of high risk activity during which the practical application of the procedures is examined in detail.

- Each visit concludes with the sending of an email highlighting identified best practices and areas for improvement.

Since 2025, the Risk and Compliance department has strengthened its level 2 controls by setting up a structured monitoring file, populated by the Regional Risk and Compliance Managers for each country in their region. This file incorporates key indicators to assess the level of implementation of the compliance program and to test its effectiveness through a sample of transactions.

The checks carried out include:

- The rate of signature of the procedures and the Code of Conduct by the employees concerned;
- The review of declared conflicts of interest, in order to identify and mitigate any potential risk;

- Reviewing gift declarations and invitations to ensure compliance with the rules in force;
- Verification of the integration of new third parties created in the ERP to the third party integrity review platform, thus ensuring a systematic assessment of their compliance.

This system aims to ensure a rigorous and consistent monitoring of the application of ethical rules and to strengthen the control of risks related to the Group's activities.

Key monitoring indicators		2023	2024	2025
Establish a site visit program	Number of entities visited	9	6	0

The third party review mechanism

All third parties with whom the Exclusive Networks group intends to initiate or continue a business relationship are subject to a specific and appropriate onboarding process, aimed at determining the level of potential corruption risk posed by each third party, and implementing the necessary mitigation measures to ensure compliance with the ethical standards that the Group has set for itself.

Accessible to all employees, this system makes it possible to quickly identify whether, in the absence of any negative signal, the risk is low, or conversely if a risk in terms of corruption or ethics is detected. When the tool detects negative signals, the third party concerned is considered "at risk": additional checks are then initiated and submitted to the validation of the Risk and Compliance Department and the Country Manager concerned.

Since 2023, the Group developed the process and included:

- updating internal and external questionnaires to conform to evaluation best practices;
- creating two new categories of third parties (payment agents and charities);
- updating the approval process; and
- implementing e-learning training for high-risk third parties.
- Implementing e-learning module for all employee to explain the importance of the onboarding process and e-learning for approvers

Key monitoring indicators		2023	2024	2025
Assessment of the integrity of third parties with whom the Group has or will enter into a business relationship	Number of third parties evaluated in the integrity tool	11,962	19,036	21,128
	Number of moderate or high risk third parties who have formally endorsed the Code of Conduct	512	1,190	310

Communication, awareness and training actions

Since 2015, compliance training has been provided several times a year:

- by the Risk and Compliance Department, in particular during seminars organised in person and more occasionally during the year, during face-to-face or online meetings;
- by the Ethics Champions, directly with their local teams, after having themselves been trained by the Risk and Compliance Department; and
- by the Risk and Compliance Department, when a new Chief Financial Officer or Country Manager is integrated.

The training courses organised by the Risk and Compliance Department are adapted whenever possible to the functions of the participants (marketing, finance, General Management or Ethics Champions). The training courses organised by the Ethics Champions are most of the time common to all employees in the region, based on the training materials prepared by the Risk and Compliance Department.

In 2025, the Risk and Compliance department continued to roll out its training plan aimed at strengthening the Group's culture of ethics and compliance. The plan included:

- Training of all employees by the entity's Ethics Champion;
- Training of Ethic Champions;
- Training with internal control as part of the integration process for new CFO or Country Manager (Country Managers)
- Development of e-learning with the creation of an e-learning module dedicated to onboarding process, as well as the presentation of procedures and tools of the compliance program.
- Training provided by the Risk and Compliance department, in person as part of site visits and/or specific requests, depending on the operational needs of the entities;

Key monitoring indicators		2022	2023	2024	2025
Employee training on ethics and anti-corruption	Number of training sessions	45	108	67	16*
	Number of onboarding sessions conducted with internal control *	13	10	14	7
	Number of Ethics Champions training courses	1	1	1	5
	Proportion of employees who have certified the Code of Conduct ***	76%	79%	81%	85%

* The reduction in the number of sessions reflects a change in delivery format rather than reduced coverage, complemented by a fivefold increase in Ethics Champions training.

** Onboarding: integration process of new Chief Financial Officers or Country Managers.

*** Employees who left the Group during the period may have been accounted for as not having certified the Code of Conduct or the alert procedure.

Whistleblowing system

In accordance with the whistleblowing procedure, employees are invited to report to the Group facts that may constitute conduct that contravenes the principles of the Code of Conduct, in particular in cases of corruption.

To this end, the Exclusive Networks group has set up an alert system in all the countries where it operates, allowing each employee and external collaborator to send a report in a confidential and secure manner, accessible from the websites.

This system complements the other reporting channels within each Group company, such as the line manager, the Human Resources Department, the Legal Department, etc.

All reported alerts are treated confidentially under the supervision of the Group's Ethics Officer, ensuring the principle of no sanction or retaliatory measure for any person who issues an alert in good faith. This principle is guaranteed by the Group and reaffirmed in the whistleblowing procedure.

Key monitoring indicators		2022	2023	2024	2025
Establish a procedure and a system for collecting and processing whistleblowing, allowing employees and third parties to report situations that are contrary to the Code of Conduct, or that may constitute a crime, an offence or a threat to the public interest	Proportion of employees certified ¹ to the whistleblowing procedure ²	62%	76%	77%	83%

1 Certified: Refers to employees who have acknowledged receipt of the procedure and have successfully passed the comprehension test.

2 Employees who left the Group during the period may have been counted as not having certified the Code of Conduct or the whistleblowing procedure.

All alerts are of internal origin, with no alerts from an external stakeholder identified in 2025.

Managing the compliance programme

Audits are regularly conducted jointly by the Group's internal audit department. They carry out tests and interviews to identify risky practices or any deviations observed as well as corrective actions to be taken.

The Exclusive Networks group has set itself the objective of having all countries subject to an audit including an anti-corruption component at least every 5 years, with the net margin of the entities covered by the audit plan representing 30% of the Group's net margin.

Key monitoring indicators		2022	2023	2024	2025
Monitoring, follow-up and evaluation of the implementation of the Group's compliance program	Number of entities covered by an audit with an anti-corruption component	14	13	12	15
	Number of proven cases of identified corruption	0	0	0	0
	Number of employees dismissed or disciplined for corruption	0	0	0	3
	Number of convictions for corruption against the Exclusive Networks group, or one of its subsidiaries	0	0	0	0

In 2025, the Group's anti-corruption audit programme covered 15 countries, consistent with the objective of subjecting all countries to review at least every five years. Two situations arose during the year that required heightened involvement from the risk and compliance team.

8.3 Transparency and the fight against tax evasion

Organisation of the tax function

The Exclusive Networks group's tax department is organised around a central team, integrated into the Group's Finance Department, which relies on local finance teams and external advisors to ensure that the Group pays taxes due in the jurisdictions in which it operates and that risks are identified, assessed and controlled.

The tax department's mission is to ensure compliance with applicable local and international tax laws and regulations, to minimise tax exposure by managing tax risk, to limit double taxation and to benefit from the tax incentives or concessions to which the Group is entitled.

Compliance, Transparency and Fiscal Accountability

The Exclusive Networks group has offices in 50 countries. Due to the global and cross-border nature of its distribution business and the complexity of the international tax environment, the Group faces uncertainties and tax risks inherent in its business.

This is due to the multiplicity and complexity of tax regulations, both local and international (including transfer pricing rules and principles governing the application of withholding taxes), and their interpretation in each country.

In this global and complex environment, the Exclusive Networks group aims to comply with all applicable tax rules and regulations in the countries where it operates, ensuring that the right amount of tax is paid in the jurisdictions where it generates profits and value. As such, Exclusive Networks is committed to complying with local and international rules, including the "OECD Transfer Pricing Guidelines for Multinational Enterprises and Tax Administrations". Exclusive Networks handles tax-related matters with integrity and does not engage in any artificial tax schemes.

In addition, each of the Group's locations abroad aims to expand the Group's activities by ensuring a local presence when operational and commercial needs require it.

8.4 Export Controls

As an international Company and considering the nature of the goods and services it markets, the Exclusive Networks group implements all necessary measures to comply with applicable laws and regulations relating to:

- export control of goods and technologies that can be used for more than one purpose;
- trade restriction measures against certain countries subject to sanctions or embargoes, decided by the United Nations Security Council, the United States via OFAC (Office of Foreign Assets Control), or the European Union in the context of foreign and security policy decisions (CFSP).

Given the nature of the products and solutions on the market, which are suitable for dual-use because they incorporate encryption technology, the cybersecurity sector is sensitive and subject to these regulations and controls.

The Exclusive Networks group operates globally in compliance with these laws, which are often extra-territorial in scope, cumulative, and regularly evolving. Their objectives are to preserve global geopolitical balances, international, national or regional security, and to combat the diversion and proliferation of certain

materials. Export control compliance is therefore an important matter for the Group.

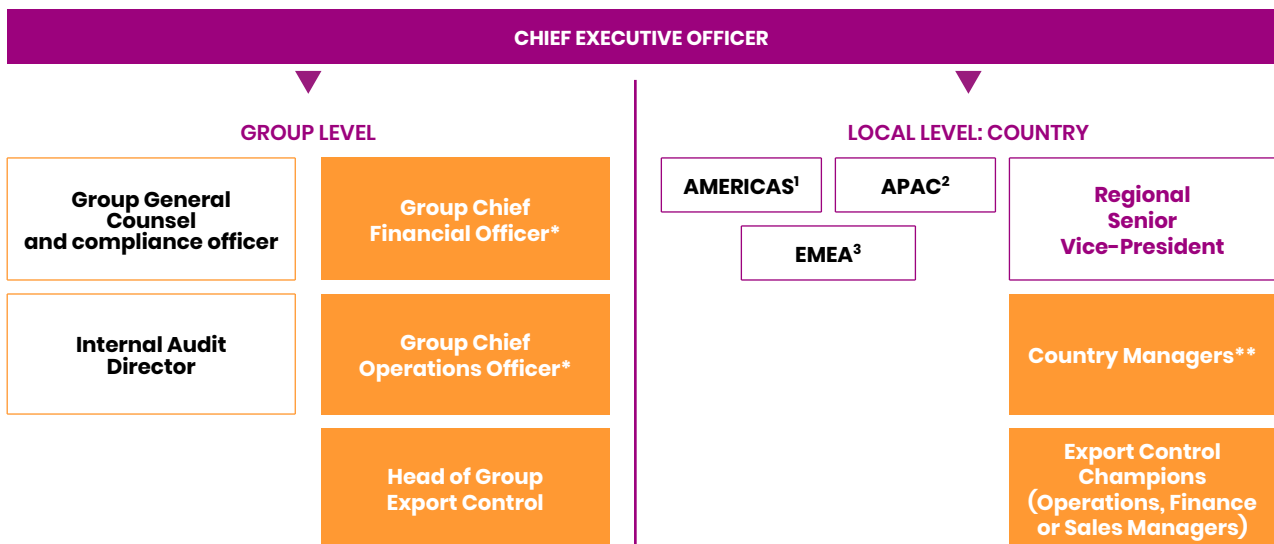
The Group applies these control regimes in all the countries in which it operates, and more specifically:

- in the European Union, in accordance with EU regulation (EU) 2021/821 of 20 May 2021 establishing the Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items;
- in the United States, in accordance with the EAR (Export Administration Regulations);
- in Singapore or the United Kingdom, in accordance with applicable local regulations.

Since the export or re-export of certain equipment is subject to the prior obtaining of an export licence or an exemption granted by the authorities of the exporting countries, the Group is informed at all times by suppliers of restrictions on the goods and services supplied. To do this, they have a dedicated organisation, which allows them to exercise strict control over their manufacturing and sales processes, in order to comply with these same obligations.

Export Control Organisation in the Exclusive Networks group

To address these challenges in a context of strong international expansion, the Group has maintained its organisation as represented below. In addition, the Internal Compliance Programme (ICP) is applied and is continuously adapted to reduce and control these risks.



■ Function in charge of export control reporting to the Chief Executive Officer.

○ Other stakeholders in the Group export control organisation

* Function with legal responsibility for export control by delegation from the Chief Executive Officer.

** Function with legal responsibility for export control of local entity

Local operational entities:

1 AMERICAS: Canada, United States.

2 APAC: Australia, Hong Kong, India, Indonesia, Malaysia, New Zealand, Philippines, Singapore, Thailand, Vietnam.

3 EMEA: Austria, Belgium, Bosnia & Herzegovina, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Ireland, Israel, Italy, Kenya, Latvia, Lithuania, Mauritius, Morocco, Netherlands, Norway, Poland, Portugal, Qatar, Romania, Saudi Arabia, Serbia, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, United Arab Emirates, United Kingdom.

The first line of risk management is made up of the Country Managers and Export Control Champions of the Group's main subsidiaries. The second line of risk control is provided by the Group Export Control Manager, who defines the export control strategy and associated procedures, and ensures regulatory monitoring, which is particularly critical given the geopolitical situation and the speed with which sanctions regimes are evolving.

The *Internal Compliance Programme*:

- is the reference framework of procedures to be followed by the Group and its subsidiaries to comply with applicable regulations, including the procedure for drawing up the declaration of final destination and end use;
- incorporates training components;
- refers to other internal procedures of the Group, such as the third-party screening system ("My TrustedPartner" platform).

In addition, the Group regularly conducts audits, either by the internal audit Department or by independent firms.

Following the previous exercise, major actions have evolved with the appointment of the Export Control Group Manager.

The main improvement measures implemented include:

- updating the Group's Export Control policy
- process review (know your end-user, resellers, etc.);
- the strengthening of coordination between the Export Control Champions with the implementation of regular communications and the coordination of the Export Control Champions network, its training and the systematic implementation of an export control clause in the Group's distribution and sales contracts; and
- the review of key export control points in coordination with the Group's internal control Department.

Awareness, training and ethical culture

Exclusive Networks deploys Export Control-related training and awareness initiatives targeting employees whose roles expose them to Export Control and sanctions risks, including sales, procurement, logistics, compliance and management functions.

Local compliance stakeholders, including Export Control Champions and Regional Risk and Compliance Managers, play a key role in promoting awareness, supporting adherence to Export Control requirements and relaying guidance at local level. Through these actions, the Group seeks to ensure compliance with Export Control regulations, embedded in day-to-day business practices.

Reporting, escalation and remediation

Exclusive Networks has established internal mechanisms to ensure the effective reporting, escalation and remediation of potential Export Control and sanctions-related non-compliance. Export Control compliance is monitored on an ongoing basis through operational controls, transaction screening and periodic reviews, enabling the identification of potential breaches or weaknesses.

Any suspected or identified Export Control non-compliance may be reported by employees through established internal reporting channels, including escalation to local Export Control Champions, Country Managers or Regional Risk and Compliance Managers, depending on the nature and severity of the issue. These reports are systematically escalated to the Group Export Control Manager, who assesses the situation and determines the appropriate course of action, in coordination with the Risk and Compliance function and, where relevant, executive management.

Where potential breaches are confirmed, the Group implements corrective and remediation measures proportionate to the identified risks. These may include transaction suspension, process adjustments, additional controls, targeted training or disciplinary measures, as appropriate. Significant incidents and remediation actions are monitored to prevent recurrence and to continuously strengthen the Group's Export Control framework. In case of non-compliance, information is flagged in screening tools to prevent, and a follow-up is done by the Group Export Control Manager, and the Internal Audit team.

Strategic relevance of export controls

Export Control compliance is a critical component of Exclusive Networks' risk management and governance framework. Given the global scale of its operations and the nature of the products and solutions it distributes, many of which incorporate advanced encryption technologies and are therefore classified as dual-use items, the company operates within a highly regulated environment requiring rigorous oversight and adherence to international trade regulations.

The Group identifies and assesses Export Control related risks as part of its compliance and risk management processes, including through the screening of transactions, End Users, destinations and third parties, with particular attention to high risk geographies, technologies and customer segments.

9 Methodological note

This methodological note describes the approach used by Exclusive Networks to calculate and report its greenhouse gas (GHG) emissions for the 2025 reporting year. The objective is to ensure transparency, consistency, and comparability of emissions data over time, in line with international standards and regulatory expectations.

The carbon footprint has been prepared in accordance with the GHG Protocol Corporate Accounting and Reporting Standard, which serves as the primary reference framework for organizational boundary definition, scope classification, and calculation principles. Emissions are expressed in metric tons of CO₂ equivalent (tCO₂e) using recognized global warming potentials (GWPs).

9.1 Scope of consolidation

The scope of the present GHG emissions report for the 2025 financial year covers 50 countries. This reporting scope includes all Group entities operating in each of the following countries:

Australia, Austria, Belgium, Bosnia & Herzegovina, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Kenya, Latvia, Lithuania, Malaysia, Mauritius, Morocco, Netherlands, New Zealand, Norway, Philippines, Poland, Portugal, Qatar, Romania, Saudi Arabia, Serbia, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Thailand, Turkey, UK, United Arab Emirates, USA, Vietnam

Collectively, these 50 countries represent almost 100% of the Group's consolidated revenue and total workforce.

The consolidation scope is applied consistently across all environmental, social and governance information published within the voluntary disclosure, including the greenhouse gas emissions inventory. Any exclusions from the reporting perimeter are justified on the basis of demonstrated non-materiality.

9.2 Preparation and compilation of this voluntary non financial disclosure

This report is published on a voluntary basis. Following its take-private transaction in March 2025, Exclusive Networks is not subject to the disclosure obligations of the Corporate Sustainability Reporting Directive (CSRD), and this report has not been prepared in accordance with the European Sustainability Reporting Standards (ESRS) or the VSME standard.

In structuring this report, the Group has nonetheless drawn on certain ESRS principles and presentation conventions, in particular the topic architecture, the double materiality approach, and the principles relating to governance, data quality and the reliability of reported information. Where individual sections refer to an ESRS standard, that reference indicates the source of inspiration for the disclosure or the terminology used; it does not indicate that the disclosure has been prepared in accordance with that standard, and it should not be read as a statement of conformity, whether express or implied.

The level of alignment with the ESRS therefore varies across topics and indicators, and certain ESRS disclosure requirements and datapoints are not covered. The Group's purpose in adopting this approach is to build a consistent and auditable reporting history ahead of any future regulatory obligation, and to respond to the ESG due diligence expectations of its vendors, financing partners and customers.

A defined selection of quantitative indicators, listed in Appendix 1, has been subject to a limited assurance engagement by an independent third party. All other information in this report is unaudited.

Where possible, the indicators and information in this report are prepared in accordance with the Guidelines of the Global reporting Institute (GRI), the Sustainability Accounting Standards Board (SASB), the recommendations of the Task Force on Climate-Related Financial Disclosures (TCFD) and the United Nations Sustainable Development Goals (UNSDGs).

Social Information

The methodology supporting the social information is designed to ensure that reported information provides a fair, balanced and understandable representation of the Group's material impacts, risks and opportunities related to its workforce.

Scope of reporting : The scope of social information covers the Group's own workforce, as defined by ESRS S1, and includes all employees of fully consolidated entities during the reporting period. Employees are included regardless of contract type (permanent or fixed-term), including apprentices and trainees.

Temporary agency workers and external service providers are excluded from workforce metrics and indicators, as they do not fall within the scope of the Group's own workforce under ESRS S1.

Unless otherwise specified, data is reported for the entire reporting year and covers all Group entities within the Group's consolidation perimeter.

- **Data sources and collection systems** : Social data is collected using a combination of centralized digital systems, ensuring consistency across geographies and business units:
 - Human resources data (e.g. headcount, workforce composition, diversity indicators) is collected through the Group's Human Resources Information System (Workday) and submitted via a collaborative sustainability reporting platform.
 - Health, safety and working conditions data, including occupational accidents, and collective agreements, is collected via a collaborative sustainability reporting platform, enabling structured data input, validation workflows and documentation of assumptions.
 - Training records are extracted from a dedicated platform connected to the Group available trainings.
- **Data quality, controls and validation** : The Group has implemented internal controls over social data collection and consolidation, including:
 - defined roles and responsibilities at local and Group level;
 - automated and manual validation checks within reporting systems;
 - consistency checks between HR, and financial consolidation scopes; and
 - management review prior to final validation and publication.

These controls are intended to support the reliability and traceability of social information and to facilitate future external assurance.

Comparability and limitations : The Group aims to ensure year-on-year comparability of social indicators by applying consistent methodologies and definitions. Where changes occur (e.g. scope, systems, methodologies), they are disclosed and explained.

Any known limitations related to data availability, estimation or coverage are identified to allow users of the report to properly interpret the information disclosed.

9.4 GRI correspondance table and alignment with SDGs

Statement of use	Exclusive Networks has reported the information cited in this GRI content index for the period from January 1, 2025, to December 31, 2025 with reference to the GRI Standards.. [GRI 2-3]		
GRI 1 used	GRI 1: Foundation 2021		
GRI Standard	Themes	Sections	SDGs
GRI 2: General Disclosures 2021	2-1 Organizational details	1 Business model	
	2-2 Entities included in the organization's sustainability reporting	9.1 Scope of consolidation	
	2-3 Reporting period, frequency and contact point	9 Methodological Note	
	2-4 Restatements of information	9 Methodological Note	
	2-5 External assurance	10 Opinion of the Independent Notified Body	
	2-6 Activities, value chain and other business relationships	1 Business model 8.4 Export Controls	
	2-7 Employees	7.1 Company Workforce	5.1, 5.5, 8.5, 10.2, 10.3, 10.4
	2-9 Governance structure and composition	3.2 and 3.2.1 Governance Structure and Oversight	
	2-10 Nomination and selection of the highest governance body		
	2-11 Chair of the highest governance body		
	2-12 Role of the highest governance body in overseeing the management of impacts		
	2-13 Delegation of responsibility for managing impacts		
	2-14 Role of the highest governance body in sustainability reporting		
	2-15 Conflicts of interest	8.2 Ethics, prevention and the fight against corruption	16.5
	2-16 Communication of critical concerns	8.2 Ethics, prevention and the fight against corruption	16.5
	2-17 Collective knowledge of the highest governance body	3 Governance Framework	16
	2-18 Evaluation of the performance of the highest governance body		
	2-19 Remuneration policies	7.4 Ensuring fair and attractive remuneration and benefits	8
	2-20 Process to determine remuneration	7.4 Ensuring fair and attractive remuneration and benefits	8
	2-21 Annual total compensation ratio		
	2-22 Statement on sustainable development strategy	2 Sustainability strategy 2024-2030	12
	2-23 Policy commitments	Sections 6, 7, 8	8

Methodological note

GRI Standard	Themes	Sections	SDGs
GRI 2: General Disclosures 2021	2-24 Embedding policy commitments	8.1 Compliance Governance & Organization	
	2-25 Processes to remediate negative impacts	8.2 Ethics, Prevention and Fight Against Corruption	
	2-26 Mechanisms for seeking advice and raising concerns	8.2 Ethics, Prevention and Fight Against Corruption	16
	2-27 Compliance with laws and regulations	8.1 Compliance Governance and Organisation	
	2-28 Membership associations	N/A	16
	2-29 Approach to stakeholder engagement	4 Analysis of material Impacts, Risks and Opportunities (IROs)	
	2-30 Collective bargaining agreements	7.3 Social Dialogue and Engagement	
GRI 3: Material Topics 2021	3-1 Process to determine material topics	4 Analysis of material Impacts, Risks and Opportunities (IROs)	7.2, 7.3, 7.a, 13.1, 13.2, 16
	3-2 List of material topics		
	3-3 Management of material topics	Sections 6, 7 and 8	
GRI 203: Indirect Economic Impacts 2016	203-2 Significant indirect economic impacts	2 Sustainability strategy	16
GRI 205: Anti-corruption 2016	205-1 Operations assessed for risks related to corruption	8.2 Ethics, prevention and the fight against corruption	16
	205-2 Communication and training about anti-corruption policies and procedures		16
GRI 302: Energy 2016	302-1 Energy consumption within the organization	6 Environmental Information	7.2, 7.3, 7.a, 13.1, 13.2
	302-3 Energy intensity		13.1, 13.2
	302-4 Reduction of energy consumption		13.1, 13.2
	302-5 Reductions in energy requirements of products and services		7.2, 7.3, 7.a, 13.1, 13.2
GRI 305: Emissions 2016	305-1 Direct (Scope 1) GHG emissions	6 Environmental Information	13.1, 13.2
	305-2 Energy indirect (Scope 2) GHG emissions		
	305-3 Other indirect (Scope 3) GHG emissions		
	305-4 GHG emissions intensity		
	305-5 Reduction of GHG emissions		
GRI 306: Waste 2020	306-2 Management of significant waste-related impacts	6.4 Resource use and circular economy	12
GRI 401: Employment 2016	401-1 New employee hires and employee turnover	7.1 Company workforce	5.1, 5.5, 8.5, 10.2, 10.3, 10.4
GRI 404: Training and Education 2016	404-1 Average hours of training per year per employee		
	404-2 Programmes for upgrading employee skills and transition assistance programmes		
	404-3 Percentage of employees receiving regular performance and career development reviews	7.5 Career and Skills Development	4.3, 4.4, 4.5

GRI Standard	Themes	Sections	SDGs
GRI 405: Diversity and Equal Opportunity 2016	405-1 Diversity of governance bodies and employees		
	405-2 Ratio of basic salary and remuneration of women to men	7.7 Diversity, Equity and Inclusion	5.1, 5.5, 8.5
GRI 414: Supplier Social Assessment 2016	414-1 New suppliers that were screened using social criteria	8 Corporate culture and business conduct policies	16

9.5 SASB correspondance table

The following table compares our reporting requirements with SASB indicators in software and computer services and hardware standards.

Topic	Accounting metric(s)	SASB code	Section
Environmental footprint of hardware infrastructure	(1) Total energy consumed, (2) percentage grid electricity, (3) percentage renewable	TC-SI-130a.1	6.3 Climate change
Data privacy & freedom of expression	Description of policies relating to behavioural advertising and user privacy	TC-SI-220a.1	7.9 Consumers and End-users; 8.1 Compliance Governance and Organisation
	Number of users whose information is used for secondary purposes	TC-SI-220a.2	Not Applicable. Exclusive Networks does not monetize customer personal data for secondary commercial purposes.
	Total amount of monetary losses as a result of legal proceedings associated with user privacy	TC-SI-220a.3	No material losses reported during FY2025.
	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring	TC-SI-220a.5	Not Applicable. Exclusive Networks is a value-added distributor and does not operate consumer-facing communication, content or social platforms. Restrictions disclosed under Section 8.4 relate to export controls and sanctions rather than censorship or content filtering.
Data Security	(1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of users affected	TC-SI-230a.1	During FY2025, Exclusive Networks did not experience any material data breach requiring disclosure.
	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	TC-SI-230a.2	7.9 Consumers and End-users; 8.1 Compliance Governance and Organisation
Recruiting & managing a global, diverse & skilled workforce	Employee engagement as a percentage	TC-SI-330a.2	7.1 Company Workforce
	Percentage of gender and racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees	TC-SI-330a.3	7.1 Company Workforce; 7.5 Career and Skills Development; 7.7 Diversity, Equity and Inclusion
Managing systemic risks from technology disruptions	Number of (1) performance issues and (2) service disruptions; (3) total customer downtime	TC-SI-550a.1	Not Currently Reported
	Description of business continuity risks related to disruptions of operations	TC-SI-550a.2	7.9 Consumers and End-users; 8.1 Compliance Governance and Organisation