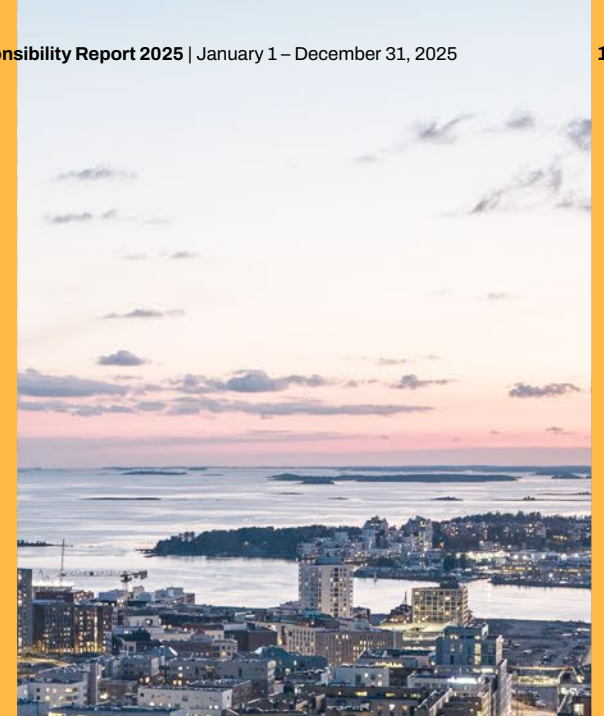




Corporate Social Responsibility Report 2025

January 1 – December 31, 2025



Contents

Greeting from the CEO	3
WithSecure 2025 Corporate Social Responsibility Highlights	4
General Information	5
About WithSecure	5
About this report	5
WithSecure's Sustainability Governance	6
Board of Directors and Board Committee	6
The Group's CEO and Global Leadership Team	6
Risk management and internal controls	6
WithSecure's Sustainability Strategy	7
Basis of the strategy	7
Business model and value chain	7
Stakeholders	8
Double Materiality Assessment	9
Climate change	9
Own workforce	10
Consumers and end-users	10
Digital trust	10
Safer and Greener Digital World	11
Cybersecurity as an enabler of greener digital ecosystems	11
Climate responsibility – identifying what matters and responding meaningfully	11
Carbon accounting and emissions data	11
Truly Equitable Workplace	13
Fair employment, inclusion and social dialogue	13
Learning, skills and meaningful work	13
Wellbeing, community and everyday support	14
Businesses Run Responsibly	15
Trust, privacy and responsible digital operations	15
Responsibility and competitive positioning	15
Strong governance and ethical business conduct	16
KPI table	17

Greeting from the CEO

In 2025, digital resilience became more than an expectation, it became a shared societal responsibility. Accelerated digitalisation, rapid AI adoption and an increasingly complex cyber threat landscape have made trust, security and resilience foundational to how societies and economies function. WithSecure exists to help organisations operate safely in this environment. Preventing harm, protecting digital infrastructure and enabling trusted digital transformation are our most important contributions to sustainability.

Protecting the digital society and preventing the damage caused by cybercrime is our most meaningful contribution to a more sustainable world. While our environmental footprint as a software company is limited, our reach is substantial. Every day we help protect millions of end-users through the organisations that trust us.

This is our first voluntary Corporate Social Responsibility report following the 2024 CSRD-aligned Sustainability Report. Although WithSecure is no longer legally required to publish sustainability disclosures, we have chosen to continue. We are in the trust business, and that means holding ourselves to a clear standard, not only in how we protect our customers, but in how we conduct our own affairs.

In 2025, we made meaningful progress across our three strategic pillars. Business flight emissions fell by 68% compared to the base year level, and total emissions remained essentially flat despite business growth. A significant milestone was reached with the decrease of the gender pay gap from 16.2% in 2024 to 7.7% in 2025. Another noteworthy accomplishment was the completion of a company-specific collective bargaining agreement in Finland, developed together with employee representatives. In addition to these, all employee training targets were met or exceeded, and 94% of employees had individual development goals in place, up from 82% the year before.

Transparency also means acknowledging where we have more to do. Our employee engagement survey pointed to areas that need attention, particularly following the organisational changes of recent years. We are listening, and a follow-up survey is planned for 2026 to measure progress. The diversity of our senior leadership also declined slightly as a result of restructuring decisions rather than by design. We take this outcome seriously and are addressing it through succession planning and how we approach recruitment going forward.

Our ambition remains unchanged, to maximise net positive impact across people, planet and digital society, grounded in transparency, materiality and long-term responsibility. For a company in the trust business, there is no more important commitment.



Antti Koskela



WithSecure 2025 Corporate Social Responsibility Highlights

Business flight emissions

decreased by 68%

from the base year level



The gender pay gap

narrowed from 16.2 to 7.7%



**NO
major
security
incidents**

according to
NIS2 directive



**WithSecure supported
humanitarian efforts
related to Ukraine**

with donations through established charitable
channels and a joint Finnish Information
Security Cluster initiative

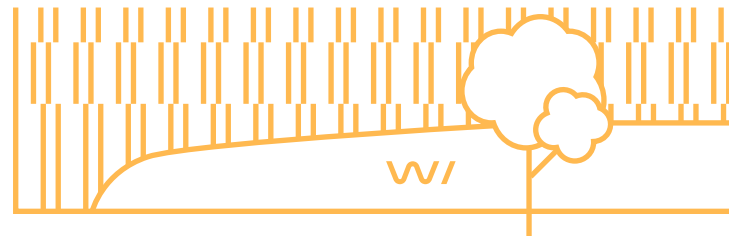


94%

of employees
had **personal
development
goals** defined
and documented

100% completion
rate

of Code of Conduct and Cybersecurity
Awareness training for new employees



General Information

About WithSecure

WithSecure is a European cybersecurity software and services company operating in the global cybersecurity industry. The company's core business is to protect organisations and their end-users from cyber threats by securing data, digital services and critical digital infrastructure. In an increasingly digital and interconnected world, cybersecurity is a fundamental enabler of economic activity, societal resilience and trust.

WithSecure's mission is to build and sustain digital trust, confidence and equity in society. This mission is guided by WithSecure's values, which emphasise integrity, responsibility, collaboration and long-term thinking. At the end of 2025, WithSecure operated across 13 locations globally and employed 593 people (headcount) representing 56 different nationalities, bringing together highly skilled experts from diverse professional and cultural backgrounds. WithSecure's people are central to the company's ability to anticipate, prevent and respond to evolving cyber risks.

Protecting the digital society and preventing damages and losses caused by cybercrime is WithSecure's most meaningful contribution to sustainable development. WithSecure's impact is primarily indirect but systemic. By enabling secure digital services, protecting privacy and data, and supporting trusted digital transformation, WithSecure can help its customers and their end-users operate safely and confidently in the digital world.

About this report

WithSecure's Corporate Social Responsibility (CSR) report covers the period from January 1 to December 31, 2025, unless stated otherwise. The information presented in this report covers WithSecure as a whole.

This report addresses environmental, social and governance (ESG) topics that are material to WithSecure, using a selected set of indicators inspired by the requirements of the Corporate Sustainability Reporting Directive (CSRD) and the European Sustainability Reporting Standards (ESRS). This reporting approach is voluntary and does not aim to be fully comprehensive. The objective of the report is to demonstrate WithSecure's commitment to continuously develop and strengthen its sustainability strategy, even though WithSecure is no longer legally required to publish sustainability related disclosures.

WithSecure's carbon footprint is calculated for the fourth consecutive year. Greenhouse gas (GHG) emissions for Scopes 1, 2 and 3 are reported in accordance with the Greenhouse Gas Protocol. The topics included in this report reflect the material impacts, risks and opportunities identified through WithSecure's Double Materiality Assessment (DMA). This report and the metrics presented have not been subject to external assurance. The targets disclosed are not science-based.

WithSecure's Sustainability Governance

WithSecure established governance principles for its sustainability programme in 2022. In 2023, the Sustainability Policy was approved as the basis of the company's sustainability work. In 2024, WithSecure actively implemented the sustainability policy objectives across the organisation, and in 2025 continued to embed those commitments into day-to-day practice. Oversight of sustainability matters is structured across three bodies: the Board of Directors, the Audit Committee, and the Global Leadership Team (GLT).

In 2025, the Global Leadership Team's gender diversity ratio (percentage of women, including CEO) was 57%.

WithSecure's Chief Financial Officer (CFO) oversees sustainability coordination and ensures that the sustainability programme is appropriately resourced. Each programme topic has a dedicated 'home team' which executes the programme as part of their broader work. The GLT is also represented in the cross-functional sustainability team that manages day-to-day sustainability operations.

Board of Directors and Board Committee

The Board of Directors is WithSecure's highest governance body and holds ultimate responsibility for sustainability matters. At the end of 2025, the Board had five members, the majority of whom are non-executive. The one executive member is an employee representative elected from the company's personnel, ensuring that employee perspectives are represented at the highest level of governance.

The Audit Committee, appointed from among Board members, supports the Board in overseeing sustainability-related targets, reporting, risk management, internal controls and policies. Sustainability is integrated into the company's business strategy and is addressed at Board meetings as and when material matters arise. The Board and its Committees review and approve sustainability priorities and objectives as well as the annual CSR report, and hold final authority over sustainability-related targets and policies.

Board composition, including its size and gender balance, changed in 2025 due to the pending acquisition of WithSecure by a consortium led by CVC Capital Partners alongside founder Risto Siilasmaa, which resulted in a reduction from seven to five members during the transaction process.

The Group's CEO and Global Leadership Team

WithSecure's management body is the CEO and the Global Leadership Team (GLT), responsible for implementing and supervising the business strategy, including the sustainability programme. At the end of 2025, the GLT had seven members, all of whom are executive members from WithSecure's personnel.

Risk management and internal controls

WithSecure's risk management approach ensures that risks related to business operations, including sustainability-related risks, are properly identified, evaluated, monitored and reported.

The Board sets the principles of risk management and internal controls, the CEO is accountable for their consistent implementation across the organisation and the Audit Committee regularly reviews top operational risks, evaluating the effectiveness of the risk management system.

Risk management extends beyond mitigation to include proactive monitoring, stress testing and opportunity identification, with the aim of building long-term strategic resilience. Internal controls are designed to provide assurance across three areas: the effectiveness and efficiency of operations, the completeness and reliability of reporting, and compliance with applicable laws, regulations and company policies.

WithSecure's sustainability due diligence is embedded in its governance, strategy and business model, ensuring the company continuously identifies, prevents and mitigates potential negative impacts across its operations and value chain, with the Board, Audit Committee and GLT actively involved and stakeholder views integrated at each key step.

WithSecure's Sustainability Strategy

Basis of the strategy

WithSecure's sustainability programme is guided by a single principle: Maximising Net Impact, on the planet, people and society. The aim is to embed sustainability into every business decision and maintain transparency with stakeholders on the company's progress.

WithSecure's most significant contribution to sustainability is its core business. By protecting organisations from cyberattacks, WithSecure helps prevent financial losses, data breaches and disruptions to digital infrastructure, all of which underpin a well-functioning, sustainable digital society.

WithSecure's sustainability strategy is guided by the W/Sustainability program, which focuses on three long-term objectives: a safer and greener digital world, a truly equitable workplace and businesses run responsibly.

Planet	People	Society
Minimise emissions from our own operations and value chain, while contributing to digital solutions that help lower systemic emissions and support efficient, secure digitalisation.	Maintain a healthy, fair, diverse and skilled workforce, ensuring safe working conditions, equal opportunities, employee wellbeing and continuous skills development to meet future cyber challenges.	Protect privacy, secure data, reduce cyber harm at scale and uphold strong ethical business conduct, reinforcing trust in digital systems and responsible business practices.

The strategy is integrated into WithSecure's overall corporate strategy and governance. As a software and services company, WithSecure's direct environmental footprint is relatively modest given the nature of its business. Nevertheless, the company is committed to minimising the environmental impact of both its products and operations, improve the sustainability of its products and services, and embed environmental and social considerations into decision-making.

WithSecure holds itself to high ethical standards across all operations. Strong emphasis is placed on ethical governance, responsible supplier practices and robust data protection. The company does not operate in the fossil fuel, controversial weapons or tobacco sectors, and has chosen not to conduct business with Russian or Belarusian parties even where permitted by export control regulations. Sustainability goals are tracked at group level, consistent with how the business is managed and reported financially.

Business model and value chain

WithSecure's business model is based on providing cybersecurity software and services to its customers. The company's clientele consists of other companies, mainly sales partners and their customers who then make up the end-user base of WithSecure's services.

WithSecure's upstream value chain consists of equipment and materials manufacturing, where for example hardware and data transmission networks for WithSecure's suppliers are processed. The value chain continues to WithSecure's suppliers who provide WithSecure with software and cloud services, equipment and third-party services, such as marketing. Moving downstream from WithSecure's own operations, which consist of digital product design and cybersecurity solutions, are WithSecure's sales partners. Lastly in the downstream value chain are WithSecure's customer companies and end-users, including their employees.

Stakeholders

The views and interests of WithSecure's stakeholders were thoroughly determined as part of the double materiality analysis. The comprehensive stakeholder interviews that were held ensured that the views and interests of the stakeholders were acknowledged. Through the identification of the material impacts, risks and opportunities, these views have been integrated into the WithSecure's sustainability programme. These stakeholders included internal experts' interviews in the double materiality assessment process.

As a part of the information gathering, the stakeholder groups' expectations for WithSecure were determined, the engagement and their possibilities of communicating with WithSecure were evaluated, and the expected outcomes as well as activities were also identified.

WithSecure's stakeholder inclusion in the double materiality analysis process highlights the company's commitment to actively listen to and engage with its stakeholders. To enable the understanding of the stakeholders' expectations and concerns, an ongoing engagement is maintained. The continuous dialogue facilitates the communication of WithSecure's sustainability efforts and processes. This enables WithSecure to align its sustainability-related efforts with the interests and views of the company's stakeholders.

The table here exemplifies WithSecure's different stakeholder groups and their sustainability-related expectations for WithSecure. The table also outlines different engagement methods and examples of sustainability related expected outcomes and activities that WithSecure undertakes.

WithSecure stakeholder	Expectations for WithSecure	Engagement	Examples of expected outcomes and activities
Employees	Fair pay and safe workplace Diversity and equal treatment Development and work-life balance	Townhalls and internal communications Training and PDPs Employee surveys Employee representative on the Board	Code of Conduct awareness Sustainability knowledge sharing PDP follow-up Pay equity assessments
Partners / Direct customers	Reliable, easy-to-use products Fair commercial models Strong collaboration and support	Partner Advisory Board Sales and technical engagement ESG support (e.g. third-party questionnaires)	Up-to-date sustainability information CO ₂ footprint data per € Improved product energy efficiency
End-customers	Reliable products Support in case of emergencies	Feedback received and improvements to products	Sharing knowledge on cyber security
Investors and financial analysts	Consistent growth Predictability of results Transparent communication Good governance	Regular meetings and presentations Capital Market Days Third-party ESG ratings	Up to date sustainability website Improvement of ESG ratings
Suppliers	Fair compensation for products/services Good business ethics	Supplier onboarding and verifications if necessary Cybersecurity scanning of IT related vendors	Develop a lean way of managing supply chain sustainability
Communities and NGOs	Responsible business conduct Contribution to digital safety Transparency	Cooperation with NGOs and initiatives Participation in awareness activities	Cybersecurity awareness initiatives Strengthening digital trust and resilience
Regulators	Compliance with regulations Transparent sustainability reporting	Advisory participation in cyber legislation Regulatory monitoring	Alignment of activities on sustainability with regulation

Double Materiality Assessment

In 2025, WithSecure updated its double materiality assessment (DMA) for the third time, reflecting the latest stakeholder expectations and the company's strategic direction.

The DMA has been carried out as an iterative process with third-party advisors. The initial materiality assessment was conducted in 2022, expanded into a double-materiality analysis in 2023, and updated again in 2024 and 2025. Regular updates enable WithSecure to better manage sustainability-related impacts, risks and opportunities and strengthen overall sustainability performance.

The DMA covers topics where WithSecure could have a material impact (inside-out approach) and those posing financial risks or opportunities (outside-in approach). Only material topics are included in this report. Both internal and external stakeholders participated in the assessment to identify material topics across the value chain, with effects quantified where applicable and supplemented by qualitative assessments where appropriate.

Stakeholder views and interests were integrated into the assessment outcomes. The administrative and supervisory bodies oversee that the operational strategy includes appropriate measures for the sustainability programme, while the sustainability team and relevant GLT members are responsible for aligning daily operations with it and managing the identified impacts, risks and opportunities.

The material topics identified fall under Climate change, Own workforce and Consumers and end-users, with additional topics related to digital trust, specifically knowledge infrastructure and knowledge creation.

Climate change

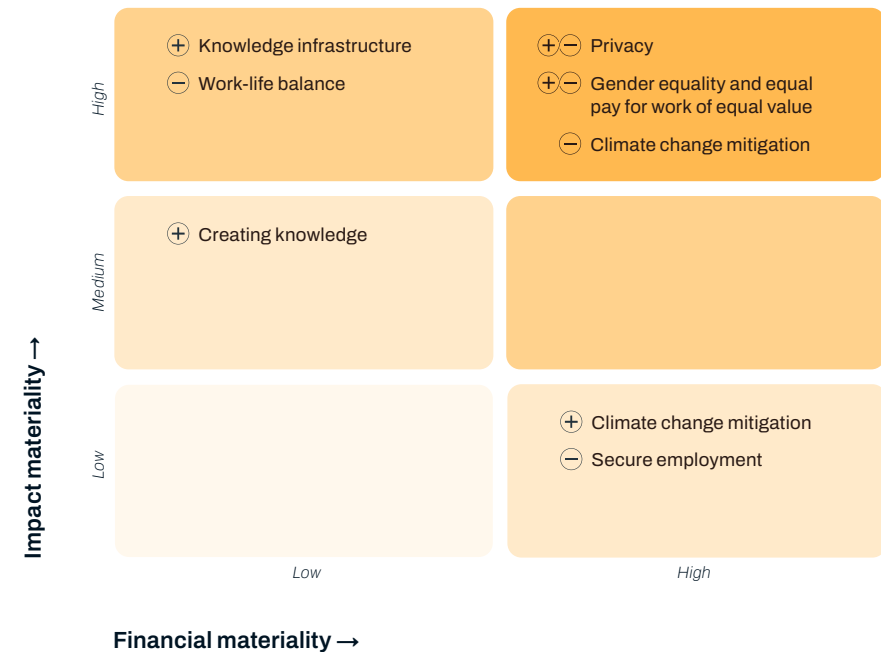
Climate change mitigation

Climate change mitigation is material for WithSecure both as a source of impact and as a business consideration. WithSecure's operations and value chain generate GHG emissions, primarily through purchased goods and services, employee commuting and business travel, which WithSecure actively works to monitor and reduce.

Growing stakeholder expectations around climate action, evolving regulatory disclosure requirements and the reputational considerations of operating as a trust-based company make a credible climate approach increasingly important. The transition to energy-efficient digital environments also creates clear opportunity. By helping customers make their cloud transitions securely and efficiently, WithSecure supports more sustainable digital operations while strengthening its own position as a trusted partner.

Financial vs Impact Materiality

⊕ — Positive materiality ⊖ — Negative materiality ⊕⊖ — Positive and negative materiality



Own workforce

Secure employment

Stable, well-supported employment is both a responsibility and a business necessity for WithSecure. High employee turnover in a cybersecurity company carries real consequences, from recruitment and onboarding costs to disruptions in knowledge continuity and service quality. Investing in a workplace where people feel valued, engaged and given reasons to stay creates genuine opportunity. Strong retention supports team effectiveness, customer relationships and long-term performance.

Work-life balance

Supporting employees' ability to balance professional and personal responsibilities is an area where WithSecure has a direct impact on people's wellbeing. Failing to do so can negatively affect long-term engagement and increase the risk of burnout and disengagement. WithSecure approaches this through flexible working arrangements, remote-work policies and a culture that supports sustainable ways of working.

Gender equality and equal pay for work of equal value

Gender equality and equal pay are among the most multifaceted material topics identified for WithSecure, spanning positive impacts, risks and opportunities. Strong female representation in senior leadership, including within the GLT, creates a positive impact by supporting more inclusive decision-making and demonstrating tangible progress. Where gender-based differences in pay and career advancement exist, they can undermine perceptions of fairness and contribute to structural inequality, while also carrying compliance and reputational risks as pay transparency regulation continues to evolve. Addressing these proactively, through salary reviews, transparent practices and a focus on equitable progression, represents a genuine opportunity to strengthen WithSecure's employer brand and its ability to attract and retain diverse talent.

Consumers and end-users

Privacy

Privacy sits at the intersection of WithSecure's core business and its broader social responsibilities. Designing products and services with strong privacy protections creates a clear positive impact: helping end-users protect sensitive information, strengthening trust in digital systems and contributing to safer digital environments at scale. Delivering those services also requires processing personal data, which creates an inherent and ongoing responsibility to protect privacy and data rights. Failures, whether in privacy-enabling solutions, data governance or regulatory compliance, could carry reputational and regulatory consequences. At the same time, WithSecure's European foundation and alignment with EU data protection standards represent a meaningful competitive opportunity, as expectations around data sovereignty and privacy-first technology continue to grow among customers and prospective employees alike.

Digital trust

Knowledge infrastructure

Through its cybersecurity expertise and solutions, WithSecure contributes to a more resilient digital knowledge infrastructure, enabling organisations and individuals to use digital systems securely and with confidence.

This positive impact extends across WithSecure's customer base and into the broader digital economy, and maintaining it is both a core responsibility and a strategic foundation of the business.

Creating knowledge

Generating, applying and sharing cybersecurity knowledge is a central positive impact of WithSecure's work. By continuously developing threat intelligence, security research and practical expertise, and making that knowledge accessible through products, services and customer collaboration, WithSecure supports long-term learning, preparedness and digital resilience across the organisations it serves and the communities that depend on a secure digital environment.

Safer and Greener Digital World

Cybersecurity as an enabler of greener digital ecosystems

Digitalisation continues to shape how organisations operate, with many replacing older, energy-intensive systems with modern cloud services. These environments are typically more efficient and can help reduce emissions, but they also depend on secure digital infrastructure. At WithSecure, cybersecurity and sustainability are closely linked. Secure and well-managed systems run more reliably and enable organisations to make full use of the efficiency benefits that modern IT provides.

Guided by WithSecure's Sustainability Policy and the results of its Double Materiality Assessment, the company's environmental work focuses on the areas where it has the most influence; managing the impacts, risks and opportunities of WithSecure's own operations, strengthening the company's understanding of value-chain emissions, and maintaining clear and consistent reporting.

Climate responsibility – identifying what matters and responding meaningfully

WithSecure's approach to climate is rooted in double materiality. Climate change mitigation is a material topic for the company, while the overall environmental impact remains limited in scope due to the nature of WithSecure's software-based business model. Most emissions arise in Scope 3 upstream activities, namely in procurement, commuting and business travel. There are no Scope 1 emissions and modest 2 emissions from leased offices.

WithSecure's business travel-related emissions decreased by 68% from the 2022 base year level, and by 61% in 2025 alone, reflecting a sustained shift in working practices and travel management.

Based on the double materiality assessment, some strategic and reputational risks have been recognised. Growing expectations for credible climate action influence WithSecure's ability to attract and retain cybersecurity talent, meet evolving regulatory requirements and maintain the trust that underpins the company's role as a security partner.

At the same time, WithSecure's double materiality assessment highlights a significant opportunity. Customers moving to modern, energy-efficient cloud environments aligns with WithSecure's role in protecting digital society. By enabling secure and sustainable cloud transitions, WithSecure can support customers' climate ambitions while strengthening its position as a trusted partner.

Carbon accounting and emissions data

WithSecure measures and reports its greenhouse gas emissions in line with the Greenhouse Gas (GHG) Protocol, applying the financial control approach. The methodology and boundaries have remained consistent throughout reporting years, ensuring comparability. Annual emissions are based on actual data for January – December where available and supplemented with estimates using historical trends where needed. While 2025 emission calculations were not externally assured, the 2024 emissions and methodologies underwent external limited assurance.

A note on cloud computing emissions

The sub-category of cloud computing and data centre services under Scope 3 Category 1 recorded a substantial increase compared to the base year level. This increase is partially explained by an update to the AWS Customer Carbon Footprint Tool methodology, which expanded the scope of reported emissions to include additional Scope 1 sources and Scope 3 categories. Historical emissions were simultaneously recalculated using these updated data sources. The methodology was third-party assured.

Due to this change in methodology, the Scope 3, Category 1, Sub-category "Cloud computing and data centre services" has been recalculated for the year 2024, for which the updated emissions data is available. The original 2024 reported that cloud computing emissions were 27 tCO₂eq, where as the recalculated corresponding emissions with the updated AWS methodology are 387 tCO₂eq. This increases the total 2024 Scope 3 Category 1 emissions from 7,915 tCO₂eq to 8,274 tCO₂eq. This has been reflected in the GHG emissions table. The base year emissions remain as is, as this updated methodology did not cover the year 2022.

While this change significantly increases the reported cloud computing figure, it represents improved emissions accounting coverage in addition to a potential increase in actual cloud-related energy use. WithSecure considers this expanded reporting scope to be a positive development in transparency and will track trends under the updated methodology going forward.

Scope 1

WithSecure does not operate assets that generate direct emissions and therefore reports no Scope 1 emissions.

Scope 2

Scope 2 emissions are calculated using both location-based and market-based methods. Calculations cover electricity and district heating in relevant European offices. Where supplier-specific emission factors are unavailable, appropriate national factors or residual-mix data are applied. Scope 2 emissions fell significantly in 2025, by 61% on a location-based basis and 52% on a market-based basis, reflecting changes in WithSecure's office portfolio.

Scope 3

Scope 3 emissions account for the majority of WithSecure's footprint. Material categories include purchased goods and services (including cloud services), waste generated in operations, business travel (flights) and employee commuting. Where suppliers provide activity-based emissions data, such as cloud service providers, these data are used directly. For other goods and services, the GHG Protocol spend-based method is applied.

Total Scope 3 emissions increased modestly in 2025 (+3% compared to 2024), with diverging trends. Business travel emissions fell sharply (-61%) and commuting emissions continued to decline (-18%), while emissions from purchased goods and services increased (+11%).

GHG Emissions Summary

		Retrospective			
		2022 (Base year)	2024 (Compa- rative)	2025	Δ% (2024 vs 2025)
Scope 1 GHG emissions					
Gross Scope 1 GHG emissions (tCO ₂ eq)		0	0	0	0%
Scope 2 GHG emissions					
Gross location-based Scope 2 GHG emissions (tCO ₂ eq)		310	928	359	-61%
Gross market-based Scope 2 GHG emissions (tCO ₂ eq)		259	630	303	-52%
Significant scope 3 GHG emissions					
Total Gross indirect (Scope 3) GHG emissions (tCO ₂ eq)		15,624	9,637	9,939	3%
1	Purchased goods and services	13,955	8,274	9,213	11%
Sub-category: Cloud computing and data centre services		26	387	359	-7%
5	Waste generated in operations	20	16	7	-56%
6	Business traveling	1,084	891	347	-61%
7	Employee commuting	565	456	371	-18%
Total GHG emissions					
Total GHG emissions (location-based) (tCO ₂ eq)		15,935	10,565	10,297	-3%
Total GHG emissions (market-based) (tCO ₂ eq)		15,883	10,267	10,242	0%

Truly Equitable Workplace

Fair employment, inclusion and social dialogue

WithSecure's people are central to its ability to protect digital society and deliver trusted cybersecurity solutions.

A truly equitable workplace is built on fair employment practices, respect for fundamental rights, and open dialogue between employees and management. At the end of the reporting period, WithSecure employed 587 full-time equivalents (FTEs). The workforce consists primarily of highly skilled professionals working under standard employment contracts.

A significant milestone in strengthening fair labour practices was achieved in Finland in 2025 with the completion and entry into force of a company-specific collective bargaining agreement, developed in close cooperation with employee representatives.

The agreement replaces the previously applied sector-level collective agreement and provides a framework tailored to WithSecure's operating model and ways of working. It strengthens transparency and predictability in areas such as working time arrangements, flexibility, compensation principles and employment terms, while remaining fully aligned with Finnish labour law and industry standards. The agreement represents a concrete outcome of active social dialogue and reinforces mutual trust between employees and management.

WithSecure maintains company-wide policies to ensure equal treatment and a safe working environment, including a Harassment Prevention Policy and Procedure, and broader non-discrimination commitments. These apply globally and are supported by accessible grievance and whistleblowing channels. In line with GDPR principles, WithSecure does not collect sensitive personal data such as sexual orientation, ethnicity or disability status, reflecting a commitment to inclusivity while safeguarding employee privacy.

Diversity, equity and inclusion efforts are supported by WIDE (Wellbeing, Inclusion, Diversity and Equity), a cross-functional employee network that promotes inclusion, wellbeing and equal opportunities.

Compensation and pay equity

Compensation practices are based on market-aligned benchmarking by role, location and skill level.

The unadjusted gender pay gap for 2025 was 7.7%, representing a substantial reduction from 16.2% in 2024.

This improvement reflects the impact of the 2025 salary review process, which included a dedicated gender pay gap analysis. WithSecure remains committed to reducing unjustifiable pay differences further, with a target of no more than 5% by the end of 2027 and continues to monitor pay equity as part of its regular salary review processes.

The unadjusted gender pay gap reflects differences in role distribution, seniority and location across the workforce. WithSecure is working to address both structural and unjustifiable elements of the gap through targeted compensation reviews, transparent salary bands and a continued focus on equitable career progression.

Leadership diversity

The proportion of other-than-male senior leaders and the number of nationalities among senior leaders both declined in 2025, falling below the target of maintaining 2024 levels. This reflects the impact of organisational restructuring during the year, which led to changes in team composition at the senior level. These changes were not directed at particular demographic groups, but their effects on the diversity profile of the senior leadership cohort are recognised. WithSecure acknowledges this gap and continues to address leadership diversity holistically through succession planning and recruitment practices.

Learning, skills and meaningful work

Continuous learning and skills development are essential to WithSecure's long-term success and to maintaining a resilient, future-ready workforce. WithSecure's learning philosophy is grounded in equal access to development opportunities and a strong focus on building capabilities aligned with the company's strategy and evolving cyber security landscape.

During 2025, employees had access to a broad range of learning opportunities combining self-directed learning, role-specific training and leadership development. Company-wide learning platforms supported continuous upskilling in areas such as AI, SaaS, leadership, customer success and emerging technologies. Leadership development remained a core focus, supported by values-based programmes and targeted learning paths for current and future leaders.

In 2025, employees completed an average of 4.6 hours of training per employee. This reflects a decrease from the 6.3 hours recorded in 2024, and falls below the target of increasing learning hours from the prior year. The decline is partly attributable to the completion of a structured onboarding and upskilling programme for a larger-than-usual cohort of new joiners in 2024, and to the effects of organisational changes in 2025 on learning continuity. WithSecure considers learning investment a priority area and will focus on strengthening learning infrastructure and participation rates in 2026.

In 2025, 93.7% of employees had documented, individualised development goals, up from 81.6% in 2024 and exceeding the target of 90%. This reflects the strengthened role of line managers in enabling personal development discussions across the organisation.

Line managers play a central role in enabling meaningful development. Regular performance and development discussions are an established practice across the organisation, providing employees with structured opportunities to reflect on goals, identify development needs and align personal growth with business priorities.

Employee engagement

In 2025, WithSecure conducted the Signi Employee Engagement Survey, with a participation rate of approximately 72%. Results indicated moderate overall satisfaction, with a general satisfaction score of 65 out of 100 and a Life-Impact-at-Work (LIT) Index score of 66 out of 100. The results highlighted areas where clarity, alignment and engagement can be further strengthened, particularly following the organisational changes of recent years.

WithSecure takes these results seriously. Survey findings were discussed across leadership forums and used to inform priorities and improvement actions. A

follow-up survey is planned for 2026 to track progress and measure the impact of actions taken. The company recognises that rebuilding strong engagement following periods of change takes consistent effort and visible follow-through and is committed to both.

Wellbeing, community and everyday support

Employee wellbeing is understood at WithSecure as a combination of physical, mental and social factors that enable people to perform meaningful work sustainably. Alongside formal policies and benefits, wellbeing is supported through everyday practices, community-driven initiatives and flexible ways of working.

WithSecure promotes work-life balance through flexible working arrangements, remote work policies and family-related leave, enabling employees to balance professional and personal responsibilities. Workplace health and safety risks remain low due to the nature of office-based work.

During the reporting period, seven minor injuries occurred in the workplace, resulting in no lost workdays, and no work-related fatalities were recorded. A global health and safety framework is in place to ensure consistent coverage across locations, addressing both physical safety and mental wellbeing. During 2025, a mandatory Safety training was launched for all employees. The training introduced WithSecure's policies, and guidance on how everyone can contribute to ensuring that all have a safe workplace.

In addition to formal structures, employee-led and community-based initiatives play an important role in fostering inclusion and connection. During 2025, initiatives such as internal networks, peer-led wellbeing activities and informal forums continued to support belonging and psychological safety. Examples include community networks focused on inclusion, mental-health awareness initiatives, and low-threshold opportunities for employees to connect, share experiences and support one another in everyday work.

By investing in learning, supporting wellbeing and strengthening social dialogue, WithSecure aims to create a workplace where people can grow professionally, feel supported as individuals and contribute to the company's long-term success in an equitable and sustainable way.

Businesses Run Responsibly

Trust, privacy and responsible digital operations

Trust is fundamental to cybersecurity and to WithSecure's role in protecting the digital society. As a trust-based cybersecurity company, WithSecure necessarily processes personal data as part of delivering effective security services. This creates an inherent responsibility to safeguard end-users' privacy and data rights across product design, service delivery, operations and the broader value chain.

WithSecure addresses this potential negative impact through privacy-by-design principles, strict data minimisation and embedded security and privacy controls in its products and internal processes. WithSecure's privacy practices are grounded in its privacy principles and Personal Data Policy, which reflect the data protection principles set out in the EU General Data Protection Regulation (GDPR). These principles guide how personal data are collected, used and protected, ensuring that data are processed only when necessary to deliver services and in a manner that respects privacy as a fundamental right.

Where products, services or tools involve the processing of personal data, privacy impact assessments are conducted to identify and mitigate privacy-related risks at an early stage. Responsibility for privacy and data protection is clearly defined across the organisation and supported by internal training, continuous product development, security testing and incident preparedness. Failures in privacy-enabling cybersecurity solutions, misuse of personal data or data breaches could undermine trust in WithSecure and weaken long-term customer relationships.

No major security incidents occurred during 2025 under the NIS2 criteria. WithSecure's ISO 27001 certification was maintained for 2025, confirming that WithSecure's information security management system continues to meet internationally recognised standards.

A key positive impact of WithSecure's operations is the enhancement of end-user privacy. By designing secure products and services with robust privacy protections, WithSecure helps customers and end-users protect sensitive information and supports trust in the digital society, contributing to safer digital environments and enabling secure participation in digital services.

Customer and partner engagement also plays an important role in maintaining and strengthening this trust. WithSecure regularly gathers feedback from customers and partners using established satisfaction and loyalty metrics, complemented by qualitative input from ongoing interactions.

Responsibility and competitive positioning

Compliance with data protection and privacy regulation is essential to maintaining trust. Non-compliance with data protection and privacy obligations could expose WithSecure to regulatory scrutiny and increased requirements related to privacy governance and controls. WithSecure mitigates this risk by aligning its practices with applicable data protection legislation, including GDPR, and by continuously reviewing and updating its privacy policies, controls and documentation to reflect evolving regulatory and industry expectations. At the same time, growing expectations around privacy, data protection and data sovereignty create strategic opportunities.

As a Europe-based cybersecurity company, WithSecure is well positioned to meet these expectations and to differentiate itself from non-EU competitors in markets where regulatory alignment, transparency and trust increasingly influence customer decisions.

Developing products that protect end-user privacy also strengthens WithSecure's attractiveness as an employer for professionals who value meaningful and responsible technology.

As digital technologies play an increasing role in business operations, WithSecure approaches their use through a strong focus on responsibility, reliability and trust. Digital solutions are applied to support secure service delivery, improve operational effectiveness and strengthen consistency across processes, while ensuring that appropriate safeguards, oversight and controls are in place. Responsible digital operations are underpinned by clear governance, well-defined roles and a disciplined approach to data use, helping ensure that technology supports business objectives without compromising security, privacy or accountability.

WithSecure also recognises that responsible digitalisation depends on human judgement and competence alongside technology. The company emphasises clear guidance, ethical considerations and role-appropriate understanding of digital tools as part of everyday work. By embedding responsibility, oversight and risk awareness into normal operating practices through policies and internal trainings, WithSecure aims to ensure that digital technologies contribute to secure, resilient and trustworthy operations, reinforce confidence among customers and partners, and support long-term value creation.

Strong governance and ethical business conduct

Robust governance and ethical business conduct underpin WithSecure's ability to manage privacy-related impacts and risks and to operate as a trusted security partner. WithSecure maintains a comprehensive set of business conduct policies, including a publicly available Code of Conduct that sets clear expectations related to integrity, compliance, anti-bribery and anti-corruption, respect for human rights and responsible business practices. These policies apply across WithSecure's own operations and its value chain and are approved and overseen by the Board.

In 2025, WithSecure achieved or exceeded all of its mandatory employee training completion rate targets across Code of Conduct, Cybersecurity Awareness and Privacy trainings.

Mandatory training supports consistent application of these principles. During the reporting period, 99% of all employees completed the Code of Conduct training, with a 100% completion rate for new employees. The Cybersecurity Awareness training was completed by 97% of all employees and 100% of new employees. The mandatory employee Privacy training completion rate was 95% for new employees and 93% for all employees.

For each training, the target completion rate is 90% for all employees and 95% for new employees. A full 100% is not always attainable due to personnel changes, leaves of absence and system reporting constraints, and the targets have been set to reflect this. Exceeding targets across all three programmes reflects the strength of WithSecure's compliance culture.

Whistleblowing protection is a key element of WithSecure's governance framework. An independent, third-party managed, confidential whistleblowing channel is available to both internal and external stakeholders, enabling the reporting of suspected misconduct.

This channel enables confidential reporting without fear of retaliation and supports the early identification, investigation and remediation of potential ethical, legal or compliance-related issues. Together this channel and WithSecure's public Whistleblowing policy are key controls for identifying and addressing potential misconduct.

Responsible supplier management supports ethical business conduct beyond WithSecure's own operations. Suppliers are required to comply with applicable laws and WithSecure's Code of Conduct, including standards related to human rights, labour practices, data protection and anti-corruption. Through supplier onboarding, risk screening and periodic reviews of strategically significant suppliers, WithSecure seeks to mitigate risks and promote responsible practices across its upstream value chain.

WithSecure also works with subcontractors for specific services. While the company's core activities rely on its own employees, subcontractors are expected to comply with WithSecure's Code of Conduct and applicable labour law standards, ensuring consistent expectations for ethical behaviour and responsible working practices.

Together, these governance practices help protect trust, reduce compliance and reputational risks, and ensure that WithSecure's business is conducted responsibly, transparently and in line with regulatory and stakeholder expectations.

KPI table

Action	Metric	Target	2024	2025
Governance				
	Board's gender diversity (% of women)		29%	0%
	Percentage of board members who are independent		86%	80%
	GLT's gender diversity (% of women, including CEO)		57%	57%
Climate change				
WithSecure commits to reducing its carbon footprint	Business flight emissions maintained at the base year level	<1084 tCO2eq	891 tCO2eq	347 tCO2eq
Own Workforce				
New investments in learning and development initiatives	Increase the total hours spent on learning per employee from the previous year		6.3 hours	4.6 hours
Support line managers in having individual development discussions	Percentage of employees that have individualised development goals defined and documented	90%	81.6%	93.7%
	Increase the representation of female leaders among the line managers		25.9%	26%
Driving diversity and promoting gender balance in leadership			35.6% other than male senior leaders	32.4% other than male senior leaders
	Maintain diversity among senior leaders at the base year level		9 nationalities	8 nationalities
Gender pay gap	Reduce the unexplainable gender pay gap by the end of 2027	5%	16.2%	7.7%
Consumers and end-users				
Awareness raising about privacy and cyber security, including informing employees	Mandatory employee Privacy training completion rate	95% for new employees 90% for all employees	93% for new employees 92% for all employees	95% for new employees 93% for all employees
	Cybersecurity Awareness training completion rate	95% for new employees 90% for all employees	100% for new employees 96% for all employees	100% for new employees 97% for all employees
Internal controls and policies kept up to date	Number of major security incidents according to NIS2 directive	No incidents	No incidents	No incidents
	Maintaining achieved certification	ISO 27001 certification achieved annually	Achieved for 2024	Maintained for 2025
Business conduct				
Awareness raising about ethical business practices, including informing own employees	Mandatory employee Code of Conduct training completion rate	95% for new employees 90% for all employees	100% for new employees 95% for all employees	100% for new employees 99% for all employees
Awareness raising about ethical supplier management, including informing own employees	Periodical supplier management reviews held with strategically significant suppliers	Held at least annually	Held during the year 2024	Held during the year 2025



WithSecure Corporation

Välimerenkatu 1
00180 Helsinki
Finland

Tel. +358 9 2520 0700
Investor-relations@withsecure.com

www.withsecure.com