Bitdefender®

REPORT

Sustainability Statement 2024

Trusted. Always.

Contents

About Bitdefender

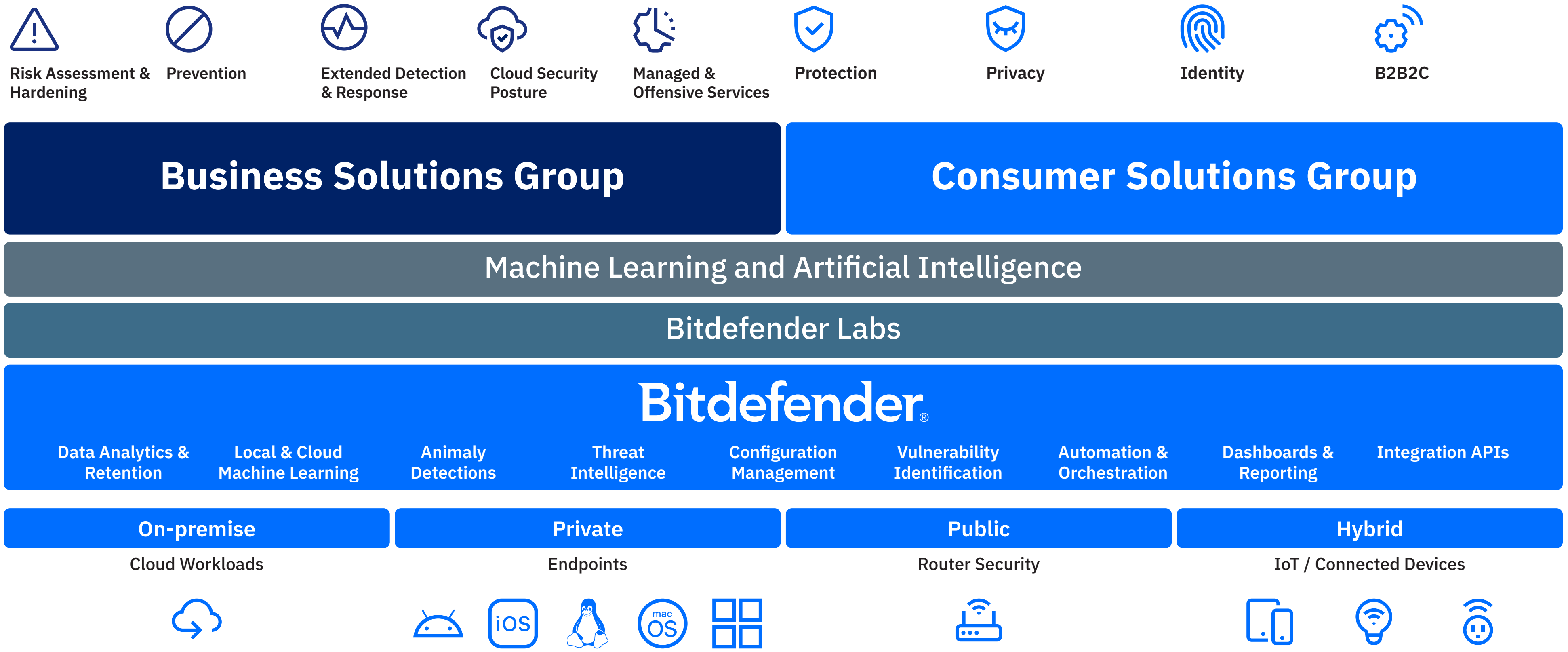
Founded by Florin Talpeș and his wife, Roxana Măriuca, shortly after the fall of communism in Romania, Softwin—the parent company of Bitdefender—became one of the country's pioneering private software firms. In 2001, Bitdefender introduced its products to the market, and has evolved into a global cybersecurity leader.

Bitdefender has strengthened Romania's standing in the global tech arena, offering a comprehensive portfolio of solutions including endpoint protection, managed and cloud security services, antivirus software, and IoT security. Its innovations, licensed by more than 200 leading global technology brands, have received numerous accolades from independent evaluators. With over 580 patents, Bitdefender continues to expand its portfolio for both enterprise and consumer markets, reinforcing its reputation as a driving force in the international security industry.

Renowned for superior protection, performance, and ease of use, Bitdefender serves a diverse client base ranging from consumers and small businesses to mid-market enterprises. Operating through two divisions - the Business Solutions Group (BSG) and the Consumer Solutions Group (CSG) - the company remains committed to its mission: deliver trusted cybersecurity solutions that empower individuals and businesses to confidently maximize digital opportunities.

Bitdefender has expanded significantly, with operations in 15+ countries, including Romania, the US, Canada, Germany, Spain, the UK, Denmark, Italy, Australia, the Netherlands, the UAE, France, alongside recent growth in Singapore, Malaysia, and Indonesia. These strategic hubs allow Bitdefender to innovate while navigating the complex regulatory demands of the cybersecurity sector.

Through its global reach - serving millions of customers in over 170 countries - Bitdefender combines international partnerships with regional expertise to deliver advanced security, drive innovation, and ensure compliance. Its key operational centers in Romania and the US position the company as a leader at the forefront of cybersecurity worldwide.



Risk Assessment & Hardening

Prevention

Extended Detection & Response

Cloud Security Posture

Managed & Offensive Services

Protection

Privacy

Identity

B2B2C

Business Solutions Group

Consumer Solutions Group

Machine Learning and Artificial Intelligence

Bitdefender Labs

Bitdefender®

Data Analytics & Retention

Local & Cloud Machine Learning

Animaly Detections

Threat Intelligence

Configuration Management

Vulnerability Identification

Automation & Orchestration

Dashboards & Reporting

Integration APIs

On-premise

Private

Public

Hybrid

Cloud Workloads

Endpoints

Router Security

IoT / Connected Devices

In 2024, Bitdefender's average global workforce grew from 1,942 employees in 2023 to 2,061 in 2024, marking a 6.1% increase. This expansion highlights Bitdefender's robust position in the cybersecurity sector. Notably, about half of the employees are engaged in engineering and research and development (R&D), illustrating a strong commitment to innovation and technological advancement.

Moreover, Bitdefender has enhanced its innovation capabilities through partnerships with Romania's top universities, supporting five R&D centers. These collaborations not only drive Bitdefender's expansion but also contribute to progress in the broader field of cybersecurity. This expansion highlights Bitdefender's robust position in the cybersecurity sector. Notably, about half of the employees are engaged in engineering and research and development (R&D), illustrating a strong commitment to innovation and technological advancement.

Bitdefender's continued growth and success remain focused on a single mission - fighting cybercrime.

ESRS 2 General disclosures

Basis for preparation

Disclosure Requirement BP-1 - General basis for preparation of sustainability statements

In preparing our 2024 sustainability disclosures, Bitdefender has chosen to report with reference to the European Sustainability Reporting Standards (ESRS), as adopted under the Corporate Sustainability Reporting Directive (CSRD). The company is not currently under any legal obligation to publish a Sustainability Statement in alignment with the ESRS. Our reporting approach was developed with particular focus on the key principles and structure of the ESRS, including:

- ↳ **Disclosure Requirements**: We have applied the relevant topical and cross-cutting disclosure requirements, with attention to transparency, consistency, and relevance in our sustainability-related data and narrative reporting.
- ↳ **Double Materiality Assessment**: In line with ESRS guidance, we conducted a double materiality assessment to identify and prioritize sustainability matters that are material from both impact and financial perspectives. This assessment has shaped the structure and content of our disclosures and governance response.
- ↳ **Governance**: Oversight of sustainability-related matters is integrated into our corporate governance framework. Responsibility for sustainability reporting, risk management, and target-setting resides with designated committees and executive functions, in accordance with ESRS governance-related requirements.

Reporting scope

As of the 2024 reporting period, no external assurance has been obtained over the sustainability data or related processes disclosed in this report. We remain committed to enhancing the robustness of our sustainability reporting and may consider external assurance in future reporting cycles.

The 2024 Sustainability Statement has been prepared on a consolidated basis, using the same scope of consolidation as the financial statements. The parent company Bitdefender Holding B.V. together with its subsidiaries are hereinafter referred as “the Group”, “Bitdefender Group” or “Bitdefender®”. Bitdefender Holding B.V. is 100% owner (direct and indirect) of its subsidiaries contained within the “Group”.

The reporting scope continues to focus primarily on direct operations, including internal policies, practices, and sustainability metrics directly managed by Bitdefender. While the current Sustainability Statement does not yet provide comprehensive coverage of the company’s upstream and downstream value chain, a first step in this direction was taken in 2024.

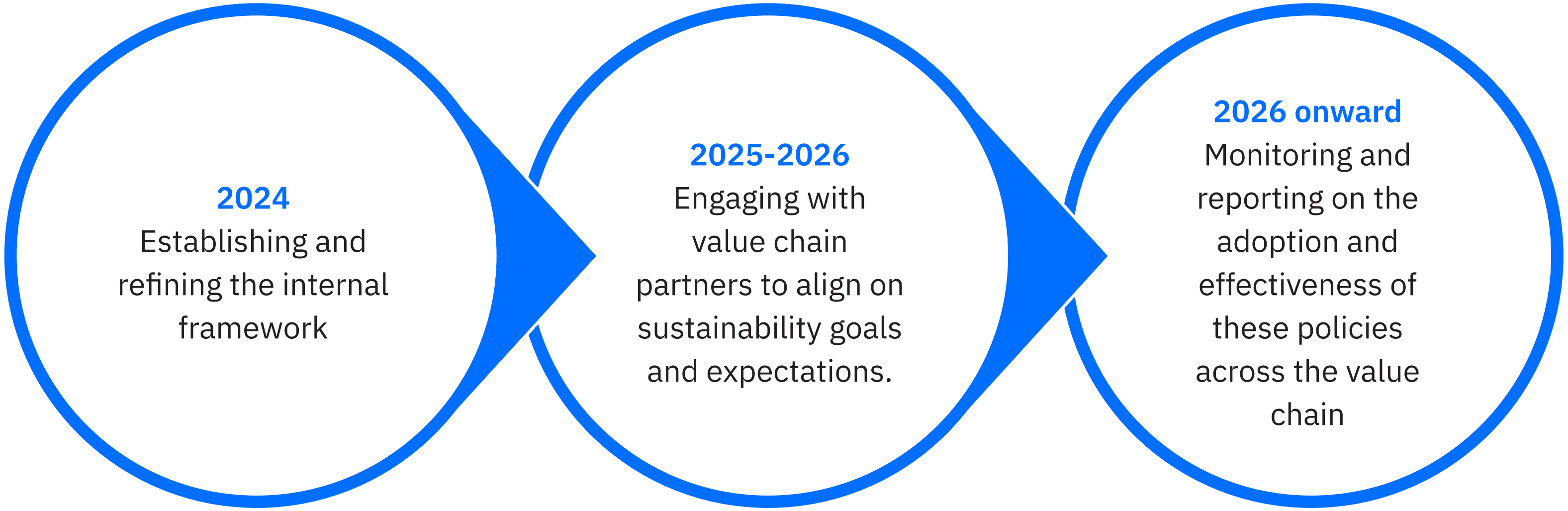
In 2024, the company conducted a Double Materiality assessment in line with ESRS requirements, extending the analysis beyond its own operations to include upstream and downstream value chain impacts, risks, and opportunities. For further details, refer to the *Impact, Risk, and Opportunity Management* section.

We acknowledge the importance of a value chain perspective for a holistic understanding of sustainability impacts. Therefore, Bitdefender is committed to:

- ↳ Initiating stakeholder engagement to map upstream and downstream impacts more effectively.
- ↳ Developing capabilities to capture and report data from suppliers, partners, and product end-of-life stages.
- ↳ Gradually aligning with ESRS recommendations as we expand our sustainability initiatives.

In the current reporting period, Bitdefender prioritized the development of a robust policies and procedures framework aimed at enhancing the integration of sustainability into its corporate strategy. This framework represents a foundational step toward embedding sustainability principles across our operations and preparing for broader application throughout the value chain.

The policies and procedures being established in 2024 are designed with scalability and adaptability in mind, ensuring they can be extended to encompass our upstream and downstream value chain. This initiative reflects our commitment to fostering sustainability practices beyond our direct operations. Bitdefender plans to roll out the application of these policies and procedures to the value chain in the coming years. The phased approach includes:



2024
Establishing and refining the internal framework

2025-2026
Engaging with value chain partners to align on sustainability goals and expectations.

2026 onward
Monitoring and reporting on the adoption and effectiveness of these policies across the value chain

For the current reporting period, Bitdefender has not used the option to omit a specific piece of information corresponding to intellectual property, know-how or the results of innovation. Furthermore, Bitdefender has not used any exemption from disclosure of impending developments or matters during negotiation, as provided for in articles 19a(3) and 29a(3) of Directive 2013/34/EU.

Use of exemption for disclosure

For specific disclosure requirements, Bitdefender has opted to apply the phase-in provisions allowed under the standards. The duration of the phase-in period ranges from one to three years, depending on the respective metric. Instances where a phase-in has been applied are detailed in the table below.

Table 1 - List of phased-in Disclosure Requirements

ESRS	Disclosure Requirement	Full name of the Disclosure Requirement	Phase-in
ESRS E1	E1-9	Anticipated financial effects from material physical and transition risks and potential climate-related opportunities	Omission of the information prescribed by ESRS E1-9 for the first year of preparation of its sustainability statement.
ESRS E5	E5-6	Anticipated financial effects from resource use and circular economy-related impacts, risks and opportunities.	Omission of the information prescribed by ESRS E5-6 for the first year of preparation of its sustainability statement.

Disclosure Requirement BP-2 - Disclosures in relation to specific circumstances

The 2024 Sustainability Statement has been prepared, for the first time, in accordance with the European Sustainability Reporting Standards (ESRS). This represents a substantial change from previous years, when disclosures were prepared using the Global Reporting Initiative (GRI) Standards and involves significant differences in how reported metrics are defined and calculated.

Bitdefender acknowledges that the definition and calculation of metrics, particularly those used to set targets and monitor progress, must remain consistent over time. We are currently developing sustainability-related targets and a metrics monitoring system in line with ESRS requirements, which will serve as the foundation for future reporting.

As no reporting errors have been identified in prior periods, no corrections are required or included in this Sustainability Statement. Where relevant, references to applicable legislation, regulations, and other recognized sustainability reporting standards have been integrated into the report to ensure clarity, transparency, and alignment with best practices.

The metrics disclosed in the 2024 Sustainability Statement do not include upstream or downstream value chain data estimated from indirect sources such as sector-average data or other proxies.

Time horizons

Bitdefender has chosen to align with the time horizon definitions in ESRS 1 General requirements (Section 6.4) for the following reasons:

1. Consistency with ESRS Guidelines: Adopting these standard definitions ensures our reporting aligns with European regulatory expectations, enabling comparability and compliance.w

2. Integration with Strategic Planning: These horizons correspond with Bitdefender's strategic planning and operational cycles, facilitating coherence between sustainability initiatives and broader business objectives.

- ↳ **Short-term refers** to the period adopted by the undertaking as the reporting period in its financial statements. This reflects immediate operational and financial performance monitoring.
- ↳ **Medium-term** is the time horizon from the end of the short-term reporting period up to 5 years, aligning with strategic project cycles and allowing for measurable progress toward sustainability targets.
- ↳ **Long-term** means a period of more than 5 years. This supports the company's vision for enduring environmental, social, and governance (ESG) impact.

3. Clarity for Stakeholders: Standardized definitions provide clarity for stakeholders regarding the timeline of sustainability actions and the expected impact over different periods

Sources of estimation and outcome uncertainty

When quantitative metrics could not be measured directly and had to be estimated, resulting in a degree of measurement uncertainty, the company provided an explanation of the estimation methodology used.

Table 2 - Quantitative metrics subject to estimation

Disclosure requirement	Data Point	Location in the Sustainability Statement
Disclosure Requirement E1-5 - Energy consumption and mix	37 a), b), c) ii	Pg. 51
Disclosure Requirement E5-5 - Resource outflows	37 a)	Pg. 57

Incorporation by reference

References to additional documents or references to information included in another chapter of the report are mentioned within the report, as follows:

Table 3 - List of references

Chapter	Disclosure Requirement	Reference to
General Disclosures	Disclosure Requirement IRO-1 - Description of the process to identify and assess material impacts, risks and opportunities	Bitdefender Group's Sustainability Report For 2023
ESRS E5 Resource use and circular economy	Disclosure Requirement E5-1 - Policies related to resource use and circular economy	Disclosure Requirement E1-2 - Policies related to climate change mitigation and adaptation (Environmental Policy)
ESRS S1 Own workforce	Disclosure Requirement related to ESRS 2 SBM-3 - Material impacts, risks and opportunities and their interaction with strategy and business model	Disclosure Requirement S1-4 - Taking action on material impacts on own workforce, and approaches to managing material risks and pursuing material opportunities related to own workforce, and effectiveness of those actions
ESRS S1 Own workforce	Disclosure Requirement S1-1 - Policies related to own workforce	Disclosure Requirement S1-2 - Processes for engaging with our workforce and workers' representatives regarding impacts.
ESRS S4 Consumers and end-users	Disclosure Requirement related to ESRS 2 SBM-3 - Material impacts, risks and opportunities and their interaction with strategy and business model	Disclosure Requirement S4-4 - Taking action on material impacts on consumers and end- users, and approaches to managing material risks and pursuing material opportunities related to consumers and end-users, and effectiveness of those actions.
ESRS S4 Consumers and end-users	Disclosure Requirement S4-1 - Policies related to consumers and end-users	Disclosure Requirement G1-1- Business conduct policies and corporate culture
ESRS S4 Consumers and end-users	Disclosure Requirement S4-3 - Processes to remediate negative impacts and channels for consumers and end-users to raise concerns	Disclosure Requirement S4-2 - Processes for engaging with consumers and end-users about impacts

Governance

Disclosure Requirement GOV-1 - The role of the administrative, management and supervisory bodies

The Bitdefender Group's governance structure guarantees cohesive management throughout all operations via a consolidated framework. This arrangement supports synchronized initiatives and maintains uniform governance across the organization. The Board of Directors is the highest governance body of the Bitdefender Group and, together with several key governance bodies, ensure robust oversight, strategic alignment, and compliance across all operational levels. These bodies include the Supervisory Board, Management Board, Executive Board, and the Boards of Directors for each subsidiary, which collaboratively work to uphold the Group's standards and policies, fostering a unified approach to corporate governance and decision-making.

Table 4 - Composition of Bitdefender's Governance bodies

Governance bodies	Women	Men
Supervisory Board - 7 executive members and 1 non-executive member	12,5%	87,5%
Management Board (corporate body of the holding company) - 1 executive member	100%	-
Executive Board (non-corporate body of the holding company) - 11 executive members	9,1%	90,9%

Supervisory Board

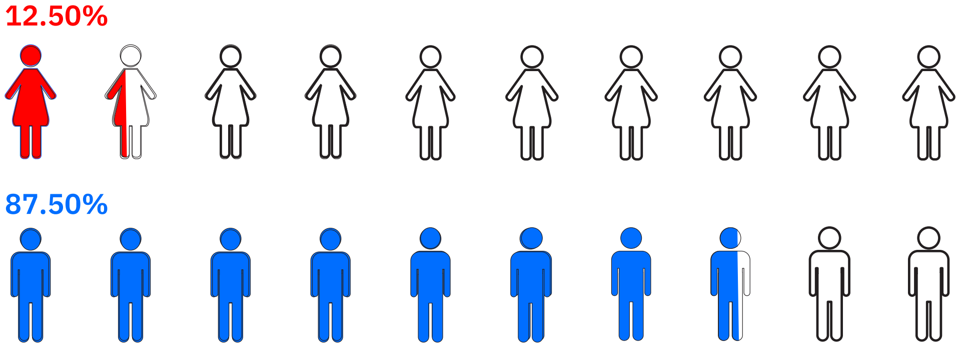
The Supervisory Board plays a central role in overseeing Bitdefender Holding B.V., acting as the top-level decision-making body and guiding the company's influence on economic, environmental, and societal factors.

Composition: The Board consists of eight members: seven executive members and one non-executive member.

Nomination & Selection: Members of the highest governance bodies and their committees are nominated and appointed in line with the Shareholders Agreement, which takes into account:

- ↳ stakeholder views
- ↳ diversity
- ↳ independence,
- ↳ candidates' competencies.

Gender representation in Supervisory Board



In addition to the Supervisory Board, the Chief Executive Officer (CEO) also holds responsibility for the oversight of the company's impacts, risks, and opportunities (IROs).

Enhancing Governance for Sustainability at Bitdefender

Since 2021, Bitdefender has prioritized strengthening the skills and expertise of its administrative, management, and supervisory bodies to effectively oversee sustainability matters. We recognize that equipping these bodies with the necessary expertise is crucial to addressing the company's material impacts, risks, and opportunities, thereby achieving our long-term ESG objectives.

1. Developing Internal Skills and Expertise

- ↳ Participation in Public Conferences
  Our ESG teams actively engage in prominent conferences and seminars, focusing on sustainability, ESG frameworks, and emerging regulatory requirements such as the Corporate Sustainability Reporting Directive (CSRD) and European Sustainability Reporting Standards (ESRS).
- ↳ Engagement with External Consultants
  We have collaborated with specialized external consultants possessing expertise in ESG reporting and compliance. This partnership provides tailored guidance and actionable recommendations to align our processes with ESRS requirements.

2. Future Investments in Training and Certifications

Recognizing the importance of internal capacity building, Bitdefender is committed to investing in comprehensive training programs designed to enhance the knowledge and skills of employees involved in ESG framework implementation and reporting. Additionally, we are exploring suitable professional certifications to support this development.

3. Commitment to Continuous Development

Moving forward, Bitdefender will continue to leverage both internal development initiatives and external expertise to ensure its governance bodies are well-equipped to address sustainability challenges and opportunities effectively. This approach reinforces the company's commitment to robust and transparent sustainability governance, aligned with the expectations of stakeholders and regulatory requirements. By combining current efforts with planned investments, Bitdefender aims to strengthen its capacity to oversee and implement comprehensive sustainability strategies and reporting processes.

Sustainability Governance and Capacity Building

Bitdefender is committed to equipping its governance bodies with the expertise needed to identify and manage significant sustainability-related impacts and risks, including climate change, regulatory compliance, and evolving stakeholder expectations. Strengthening these capabilities ensures informed decision-making that aligns with the company's strategic priorities.

Developing sustainability-related skills within governance structures is essential for improving the quality and efficiency of ESG reporting. This includes ensuring full compliance with the ESRS and delivering transparent, accurate, and reliable disclosures. Through targeted training and capacity-building initiatives, the company is enhancing its ability to monitor, assess, and report on material sustainability issues effectively.

These initiatives strengthen the company's capacity to set and achieve ambitious ESG objectives, such as reducing environmental impacts, advancing social responsibility, and upholding robust governance practices. By aligning sustainability-related skills and expertise of governance bodies with Bitdefender's strategy, the company establishes a strong foundation for long-term success and value creation.

The CEO serves as the lead executive for ESG matters, ensuring that sustainability priorities are integrated into corporate strategy. Sustainability topics are regularly discussed at senior management meetings and, where relevant, placed on the Board's agenda. Members of the Supervisory and Executive Boards bring diverse expertise in areas such as cybersecurity risk, regulatory compliance, and organizational governance. Where specialized sustainability knowledge is required, they are supported by internal ESG experts and, when necessary, external advisors.

Management's Role in Overseeing Sustainability Impacts, Risks, and Opportunities

The governance structure of Bitdefender is anchored by the Supervisory Board, the top governing body tasked with decision-making and oversight regarding the organization's impacts on the economy, environment, and society. However, the CEO, as the highest executive authority, plays a pivotal role in managing these impacts. The CEO is responsible for setting the company's strategic trajectory, which also encompasses its approach to Environmental, Social, and Governance (ESG) matters. This includes guiding the organization's commitment to sustainability, social responsibility, and ethical conduct.

The CEO is accountable for monitoring ESG-related risks that might affect the organization's performance and long-term success, encompassing potential legal, financial, and reputational challenges linked to ESG matters. To ensure ESG integration into the company's overarching strategy, the CEO collaborates with the board to align ESG targets with the firm's mission, vision, and business goals, thereby nurturing sustainable and responsible business practices. Additionally, the CEO supervises the creation and publication of ESG reports.

Disclosure Requirement GOV-2 - Information provided to and sustainability matters addressed by the undertaking's administrative, management and supervisory bodies

The governance framework at Bitdefender ensures that oversight bodies are equipped to effectively supervise and support the company's sustainability commitments. Our administrative, management, and supervisory bodies receive regular updates on sustainability through internal reporting mechanisms, formal ESG updates, and strategic oversight meetings.

Disclosure Requirement GOV-3 - Integration of sustainability-related performance in incentive schemes

The Executive Board of Bitdefender Holding BV, together with the CEO, CFO, Global HR Director and VPs of Lines of Business, validate remuneration packages for the highest governance body and senior executives. The Human Resources team provides market benchmarking data and maintains records of compensation structures to support these decisions.

Performance criteria considered in remuneration decisions include the achievement of objectives and competency evaluations, as well as assessments of critical roles and skills. Currently, performance at the governance level is not assessed based on sustainability criteria, and sustainability or climate-related performance metrics are not integrated into the incentive schemes for administrative, management, or supervisory bodies.

Disclosure Requirement GOV-4 - Statement on due diligence

Bitdefender integrates due diligence on sustainability matters into its corporate governance, policies, and risk management frameworks through several key practices:

1. Board-Level Engagement in Cybersecurity:

Recognizing cybersecurity as a critical component of enterprise-wide risk management, Bitdefender's leadership actively participates in developing and overseeing security strategies. This approach ensures that cybersecurity is not viewed merely as an IT concern but as a significant aspect of corporate governance and risk oversight. Such involvement aligns with best practices, emphasizing the importance of addressing cybersecurity within the broader context of organizational risk management.

2. Commitment to Human Rights Principles:

Bitdefender's Code of Business Conduct reflects a commitment to respecting and promoting human rights, guided by frameworks like the UN Guiding Principles for Business and Human Rights. This dedication is embedded in the company's policies and practices, ensuring that all individuals are treated with respect and dignity. By aligning its operations with these international standards, Bitdefender incorporates human rights considerations into its corporate governance and risk management processes.

3. Comprehensive ESG Reporting:

In its Sustainability Reports, Bitdefender addresses various environmental, social, and governance aspects, including:

Environmental aspects: The report covers key areas of environmental impact, including energy consumption, greenhouse gas emissions, resource efficiency, as well as waste generation and management.

Social Aspects: The report discusses topics such as social dialogue, freedom of association, equal treatment and opportunities, training and skills development, employee rights (including privacy and human rights), and the personal safety of consumers and end-users.

Governance Aspects: It covers business conduct (including organizational culture and whistleblower protection), managing supplier relationships, responsibility for sustainability in the value chain, and ethics and integrity (including anti-corruption measures).

The CEO has a pivotal role in overseeing the company's due diligence processes related to economic, environmental, and social impacts. The CEO's responsibilities include setting the strategic direction, which encompasses the development and approval of policies that ensure responsible corporate conduct and decision-making.

Additionally, Bitdefender emphasizes the importance of board-level engagement in cybersecurity, recognizing it as a critical component of enterprise-wide risk management. This approach ensures that cybersecurity is addressed within the broader context of organizational risk management, reflecting the company's commitment to integrating due diligence into its governance structures.

Disclosure Requirement GOV-5 - Risk management and internal controls over sustainability reporting

Scope, main features and components (including main risk categories)

Bitdefender has established a comprehensive Enterprise Risk Management (ERM) framework aligned with the principles of ISO 31000, encompassing both financial and non-financial risks, including those related to Environmental, Social, and Governance (ESG) matters. The framework is designed to support informed decision-making and promote sustainable business practices across the organization.

The risk management and internal control systems cover all levels of the organization and apply to the **key risk categories** identified:

Strategic Risk: Risks arising from changes in the market, technology landscape, or customer needs that may impact the company's ability to achieve its long-term objectives or maintain a competitive position.

Operational Risk: Risks related to internal processes, systems, people, or external events that could disrupt service delivery, impact performance, or compromise the integrity of cybersecurity operations.

Compliance Risk: Risks associated with failing to meet legal, regulatory, or contractual obligations, particularly in relation to data protection, cybersecurity standards, and client-specific requirements.

Reputational Risk: Risks that could damage the company's brand, stakeholder trust, or customer relationships due to perceived failures in security performance, incident response, or ethical conduct.

In the context of sustainability reporting, the scope extends to identifying, assessing, mitigating, and monitoring ESG-related risks and opportunities that may impact the company's long-term performance and stakeholder value.

Risk management processes are integrated with the company's strategy, ensuring that ESG risks are identified and addressed in alignment with organizational goals. Clear governance structures are in place, with defined roles and responsibilities for managing ESG risks, including oversight from senior management and relevant committees. The system operates on a continuous cycle of risk identification, assessment, response, monitoring, and review.

A structured set of policies and internal guidelines governs the risk management lifecycle, ensuring consistency, transparency. ESG risks are documented and evaluated using standardized tools and criteria, facilitating prioritization and response planning. Controls are embedded across business functions to mitigate key risks, while internal audit and compliance functions provide assurance on the effectiveness of controls.

Bitdefender applies a structured and systematic approach to risk assessment, embedded within its broader Enterprise Risk Management (ERM) framework. The process is governed by an internal Risk Identification, Assessment, and Control & Mitigation Procedure, which supports the full risk lifecycle—from detection to treatment and monitoring.

Risk Assessment Approach

The methodology follows the principles of ISO 31000 and focuses on identifying both current and emerging risks across operational, strategic, and ESG domains. Risks are assessed consistently across all business units using standardized tools and criteria that ensure comparability and transparency.

To support effective decision-making, Bitdefender utilizes an internal Risk Taxonomy to classify and structure risks across categories, enhancing visibility and clarity. Each identified risk is evaluated using a scoring system based on two key dimensions: **Probability of Occurrence** and **Potential Impact on Objectives**.

These scores are plotted against a Risk Matrix, which supports objective prioritization by mapping the relative severity of risks. This approach ensures that resources are focused on addressing the most critical threats and opportunities.

Risks assessed as high or significant are escalated and consolidated into a Group-wide Risk Report, which is regularly reviewed by senior leadership and relevant governance bodies. This report enables top-down oversight and ensures alignment between risk management, strategic objectives, and sustainability performance.

By following this rigorous assessment and prioritization process, Bitdefender maintains a proactive and forward-looking posture on risk, reinforcing the integrity and reliability of its sustainability reporting and broader risk governance.

Integration of findings into internal functions

Bitdefender ensures that the outcomes of its risk assessments are fully integrated into the company's internal functions and sustainability reporting processes. This integration is achieved through structured coordination between risk management, compliance, sustainability, and operational teams.

Key integration mechanisms include:

- ↳ **Cross-Functional Collaboration**: ESG-related risks identified through the formal risk assessment process are communicated across relevant departments, including HR, IT, Administration, Finance, and Legal, to inform operational practices and ensure alignment with objectives.
- ↳ **Embedded Controls**: Internal controls designed to manage ESG risks—such as those related to emissions, resource use, employee wellbeing, and waste—are incorporated into day-to-day workflows and monitored regularly for effectiveness.
- ↳ **Data Governance and Reporting**: Risk findings influence the design and refinement of data collection and reporting procedures, ensuring that sustainability disclosures are accurate, reliable, and aligned with international reporting frameworks.

↳ **Feedback into Strategy:** Insights from the risk and control environment feed into broader corporate strategy and sustainability planning, enabling continuous improvement and proactive mitigation of emerging ESG risks.

Through this integrated approach, Bitdefender strengthens the connection between its operational reality and its sustainability reporting, ensuring transparency, consistency, and strategic alignment across the organization.

Periodic reporting to administrative and management bodies

Bitdefender has a structured process for identifying, reviewing, and escalating ESG and enterprise risks to senior management and the Board. Risks are first reviewed and prioritized by risk owners, then presented to senior management on a semi-annual basis, with select categories reviewed monthly. Critical risks are escalated to the Board, where they are consolidated into a formal report reviewed by the CEO and presented to the Audit & Risk Committee twice a year, with interim updates provided mid-cycle.

This tiered approach ensures sustainability-related risks are regularly monitored, communicated, and integrated into strategic oversight. Effectiveness is assessed through audits, risk reviews, supplier evaluations, and stakeholder engagement. While no formal due diligence framework is in place, the company addresses concerns through existing feedback channels and is committed to transparency and continuous improvement.

Strategy

Disclosure Requirement SBM-1 - Strategy, business model and value chain

Business model and Value chain Overview

Bitdefender operates a value-driven, innovation-led cybersecurity business model, anchored in its ability to produce advanced threat detection technologies and scalable protection services for a global market. Its business model combines deep R&D, proprietary technologies, global partnerships, and platform-based delivery to serve both individuals and organizations, from consumers to Fortune 500 enterprises. For information regarding the company’s total number of employees and revenue, please refer to the “About Bitdefender” section.

Our value chain is built for resilience, scalability, and trust-qualities essential in today’s high-stakes digital security landscape.

At the core of our value chain are three major stages:

Input Acquisition & Development - Gathering and developing human capital, data, infrastructure, and technologies

1. **Productization & Delivery** - Converting technical capabilities into deployable products and services
2. **Outcome Realization & Feedback** - Delivering stakeholder value and using feedback loops to improve offerings
3. **Critical Stages in the Value Chain**

1. R&D and Threat Intelligence Collection (Upstream)	2. Cloud Integration and Infrastructure Scaling (Midstream)	3. Market Segmentation and Distribution Strategy (Downstream)	4. Post-Sale Customer Engagement and Support (Downstream)
Core to maintaining a technological edge	Enables real-time global delivery and resilience	Ensures customer relevance and commercial success	Drives retention, customer trust, and recurring revenue

Bitdefender is positioned at the **technological and strategic core** of the cybersecurity value chain. It connects upstream innovation with downstream delivery through:

- Advanced R&D,
- Cloud-native infrastructure,
- Robust global partnerships,
- And a keen understanding of diverse customer needs.
- Bitdefender operates primarily on a **subscription-based SaaS model**, delivering its security solutions through cloud-native platforms.

Main Revenue Streams

- Consumer solutions and security software subscriptions
- Enterprise security platforms (EDR, XDR, GravityZone)
- Managed detection and response (MDR) services
- Licensing technologies to OEMs and strategic partners
- Specialized cybersecurity consulting and incident response services

Our business model depends on continuous innovation, massive data processing capabilities, and a highly skilled workforce capable of staying ahead of rapidly evolving threat landscapes.

Bitdefender thrives within a complex ecosystem of contributors, validators, and enablers. Among these, community involvement, supplier relationships, and engagements with independent testing bodies are particularly critical to building trust, driving innovation, and maintaining market leadership

ESG
Environment
Social
Governance

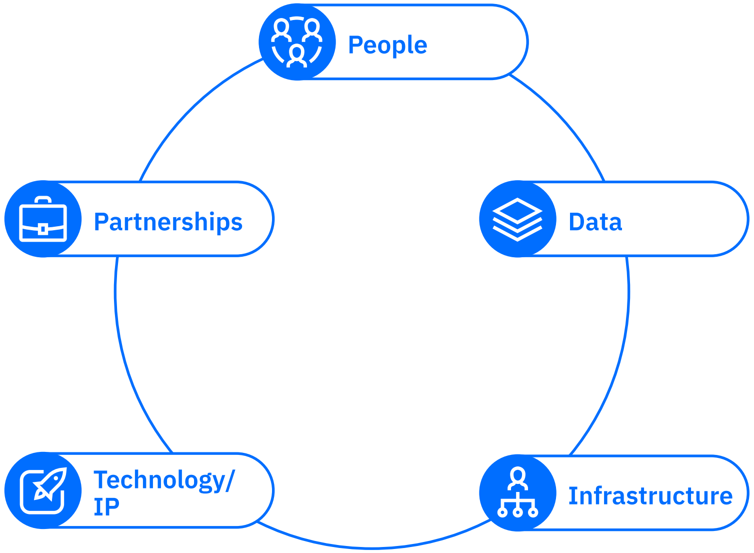
Bitdefender's interactions with communities, suppliers, and independent validators are not transactional - they are strategic collaborations that shape its products, validate its claims, and guide its innovation roadmap.

- ↳ Communities give Bitdefender visibility into the future and a feedback loop with the broader cybersecurity world.
- ↳ Suppliers act as building blocks of agility and scale, underpinned by secure and compliant practices.
- ↳ Independent testing bodies hold Bitdefender publicly accountable and help it continually refine its offering.

Together, these relationships form a resilient ecosystem that strengthens Bitdefender's position as a trusted cybersecurity provider in an era where trust, transparency, and collaboration are just as important as raw technical capability.

Inputs

At the heart of Bitdefender's ability to deliver continuous innovation and protection is a well-structured value chain, centered on five core inputs:



Bitdefender's most strategic asset is its people, particularly those with deep expertise in cybersecurity, threat research, AI, and software engineering.

Bitdefender actively recruits top talent both locally and globally, drawing heavily from Romania's strong pool of engineering graduates, especially from universities in Bucharest, Cluj-Napoca and Iași. It has established talent pipelines through academic partnerships and internships and is known for aggressively hiring experienced professionals in cyber threat intelligence, malware research, incident response, and cloud security from international markets.

Continuous development is baked into the company's culture. Bitdefender invests in internal training programs, certifications, and professional development. It encourages participation in global conferences, white-hat competitions, and research collaborations. This emphasis on skill-building ensures teams remain at the forefront of rapidly evolving cybersecurity threats.

Bitdefender employs rigorous internal access control, role-based security clearances, and behavioral monitoring to ensure that internal knowledge and capabilities are protected. Insider threat programs and security awareness training are also used to maintain a secure workforce.

Data and Information. Bitdefender relies on massive volumes of real-time threat intelligence, which it collects, processes, and uses to fuel its threat detection algorithms.

Data protection is critical to Bitdefender's credibility. All data collected is anonymized, encrypted, and stored securely across its global infrastructure. The company complies with data privacy regulations like GDPR and implements strong governance, including data classification, secure transmission protocols, and strict data retention policies.

The backbone of Bitdefender's operations is its robust infrastructure, supporting everything from cloud-based protection to research and development.

Bitdefender uses a combination of in-house data centers and global cloud providers like Google Cloud, Amazon Web Services and Microsoft Azure to maintain flexibility, scalability, and high availability. Its infrastructure supports real-time telemetry analysis, cloud scanning, and continuous delivery of threat updates.

Bitdefender builds and customizes much of its own infrastructure to support high-performance computing for malware analysis, machine learning model training, and global service delivery. Internal DevOps teams continuously optimize these systems for resilience and scalability.

All infrastructure is protected using multi-layered defense mechanisms, firewalls, encryption, zero-trust architecture, and real-time monitoring. Regular stress tests, failover drills, and disaster recovery plans ensure service continuity and threat resilience.

Bitdefender's competitive advantage lies in the proprietary technologies it has developed over two decades.

The company has a long history of in-house innovation, developing its own malware detection engines, sandboxing technologies, anti-exploit systems, and AI-driven behavioral analytics. It also acquires niche technology companies to supplement its capabilities in areas such as EDR (Emergency Detection and Response), IoT security, and cloud workload protection.

Innovation is formalized through significant investment in Research & Development, which makes up a large portion of Bitdefender's budget. The company has earned over 580 patents, many related to heuristic detection, traffic inspection, and threat remediation and machine learning. Bitdefender Labs, its R&D division, constantly experiments with new techniques for combatting evolving threats like ransomware, APTs (Advanced Persistent Threat), and supply-chain attacks.

Intellectual Property is protected through legal mechanisms (patents, copyrights) and cybersecurity measures such as secure code repositories, internal red-teaming, and role-based access to source code. Secure development practices (SDLC) and code reviews are rigorously enforced to prevent internal or external tampering.

Outputs

Bitdefender’s primary outputs are the tangible and digital deliverables that come from its R&D, engineering, and commercial operations. These include:

1. Cybersecurity Products	2. Cybersecurity Services	3. Proprietary Technologies
GravityZone Platform - an integrated suite offering EPP, XDR, EDR, Risk Analytics, and Cloud Security for enterprises. **Home security solutions** - antivirus, VPN, password managers, and parental controls for consumers.	**Managed Detection & Response (MDR)** - continuous monitoring and incident response. **Threat Intelligence Services** - delivering curated, real-time threat feeds to enterprise clients and government agencies. **Security Consulting & Risk Assessments** - helping organizations reduce the attack surface and comply with standards.	**AI**-driven threat detection engines - capable of identifying known and unknown malware. **Cloud**-based scanning and telemetry infrastructure - processing billions of signals from global endpoints. **Behavioral analysis and sandboxing tools** - forensics and real-time protection. **Patented algorithms** - recognized for accuracy, speed, and low false-positive rates.

The outcomes are the real-world impacts these products, services, and technologies generate for Bitdefender’s key stakeholder groups. These benefits are both current (realized today) and expected (strategic or long-term).

Table 5 - Current and expected benefits of Bitdefender's products and services

For Customers (B2B and B2C)	For Investors and Business Partners	For Employees	For Society and the Digital Ecosystem
Current Benefits: ↳ Enhanced protection against ransomware, APTs, phishing, and other threats ↳ Reduced downtime and operational risk through proactive defense and fast incident response ↳ Greater confidence in digital operations, especially in regulated or high-risk industries ↳ Integrated solutions that reduce security complexity and improve visibility	**Current Benefits**: Strong brand reputation built on independent test results and industry trust ↳ Revenue diversification across consumer, SMB, enterprise, and OEM markets ↳ Global footprint with operations and clients in over 170 countries	**Current Benefits**: Access to cutting-edge projects in AI, reverse engineering, and threat research ↳ Strong internal training programs and R&D culture ↳ Global collaboration across teams in Romania, the U.S., S-E Asia and other innovation hubs	**Current Benefits**: Protection of digital infrastructure for businesses, schools, governments, and healthcare systems ↳ Contributions to global threat intelligence and public cybersecurity awareness ↳ Active role in cybercrime investigations and threat disclosures
Expected Benefits: Future-proof defenses through AI-powered adaptation to new attack vectors ↳ Increased automation and lower total cost of ownership via managed services ↳ Compliance alignment through advanced reporting and risk analytics	**Expected Benefits**: Sustained growth potential, fueled by rising demand for cybersecurity across verticals ↳ Expansion into adjacent markets, such as IoT and critical infrastructure security ↳ Scalability and platform monetization via subscription and managed service models	**Expected Benefits**: Career growth and development through leadership in a high-impact, future-facing industry ↳ Participation in meaningful work with societal importance ↳ Cultural alignment with a company that values innovation, transparency, and mission-driven goals	**Expected Benefits**: Support for a safer digital society, especially as more of life moves online ↳ Alignment with digital ethics and data privacy standards ↳ Preparedness against cyberwarfare and nation-state threats, contributing to geopolitical stability

Disclosure Requirement SBM-2 - Interests and views of stakeholders

Bitdefender actively engages stakeholders through consultations and an annual survey is sent out to gather their input on sustainability topics related to the Group's operations. During these consultations, the CEO carefully reviews the opinions, concerns, and suggestions from various stakeholder groups. Bitdefender remains dedicated to maintaining open and transparent communication about its sustainability performance. Bitdefender conducts a comprehensive stakeholder analysis to identify and prioritize key groups that have a vested interest in or are impacted by its operations.

Our stakeholder engagement approach

1. Comprehensive Stakeholder Analysis:

To ensure that its sustainability initiatives align with the expectations and concerns of those affected by its operations, Bitdefender conducts thorough stakeholder analyses. This process involves identifying and prioritizing key groups with vested interests in the company's activities, including employees, customers, suppliers, communities, regulators, and non-governmental organizations (NGOs).

2. Internal Stakeholder Consultations:

Bitdefender's 2024 double materiality assessment involved engaging internal stakeholders to identify and evaluate the company's impacts, risks, and opportunities related to sustainability. For more information regarding the internal stakeholders consulted in the identification and evaluation process of the material sustainability matters, please refer to Disclosure requirement IRO-1 - Description of the process to identify and assess material impacts risks and opportunities.

Through this comprehensive engagement, Bitdefender effectively identifies and addresses sustainability-related risks and impacts, ensuring that its operations align with the expectations and needs of its diverse stakeholder base.

3. Integration of Stakeholder Feedback:

The feedback collected from these consultations is integral to Bitdefender's strategy. By carefully reviewing the opinions, concerns, and suggestions from various stakeholders, the company ensures that its Environmental, Social, and Governance (ESG) policies and procedures are both relevant and effective. This collaborative approach fosters a sense of shared responsibility and enhances the overall impact of Bitdefender's sustainability efforts.

4. Leadership Involvement:

Bitdefender's Chief Executive Officer (CEO) plays a pivotal role in steering the organization's ESG initiatives. The CEO actively engages with stakeholders through annual surveys and consultations, ensuring that their insights are incorporated into the development of ESG policies. This top-level commitment underscores the importance of sustainability within the company's corporate governance framework

5. Transparent Communication:

Maintaining open and transparent communication about its sustainability performance is a priority for Bitdefender. The company disseminates information regarding its ESG commitments and progress through various channels, including annual sustainability reports. This practice not only keeps stakeholders informed but also reinforces Bitdefender's dedication to accountability and continuous improvement

The Disclosure Requirements related to ***ESRS 2 SBM-2 Interests and views of stakeholders*** specific to the topical standards (S1 Own workforce and S4 Consumers and end-users) can be found in the dedicated chapters.

Impact, risk and opportunity management

Disclosure Requirement IRO-1 - Description of the process to identify and assess material impacts, risks and opportunities

Disclosure Requirement SBM-3 - Material impacts, risks and opportunities and their interaction with strategy and business model

Since the launch of our first Sustainability Report, Bitdefender has consistently carried out materiality assessments. In previous periods, this analysis adhered to the provisions and recommendations set forth by the GRI Standards. However, this year, modifications have been implemented to align with the CSRD and ESRS requirements concerning the Double Materiality Assessment (DMA) process.

The DMA encompasses two dimensions: **impact materiality and financial materiality**.

A sustainability matter is considered material from an impact perspective if it relates to Bitdefender's actual or potential, positive or negative impacts on people or the environment over the short, medium, or long term. These impacts may arise from the company's own operations, its upstream and downstream value chain, its products and services, or its business relationships.

A sustainability matter is considered financially material if it causes, or could reasonably be expected to cause, significant financial effects for Bitdefender. This applies when the matter gives rise to risks or opportunities that materially influence, or could be expected to materially influence, the company's development, financial position, performance, cash flows, access to financing, or cost of capital over the short, medium, or long term.

In the Double Materiality Assessment carried out for the financial year 2024, Bitdefender identified material sustainability matters from both impact and financial perspectives, as well as associated impacts, risks, and opportunities. The evaluation extends beyond the company's operations, encompassing the upstream and downstream value chain.

A sustainability matter is deemed material if it fulfills either impact materiality or financial materiality criteria - or both. For material impacts, risks, or opportunities covered by ESRS Disclosure Requirements, Bitdefender identifies and reports pertinent information in accordance with ESRS guidelines. If ESRS inadequately covers these aspects, the company develops and utilizes additional entity-specific disclosures.

The following section details the methodology employed to identify impacts, risks, and opportunities, assess their materiality, and form the basis for disclosures in Bitdefender's sustainability statement. The Disclosure Requirements related to ***ESRS 2 SBM-3 Material impacts, risks and opportunities and their interaction with strategy and business models*** specific to the topical standards (E1 Climate change, S1 Own workforce and S4 Consumers and end-users) can be found in the dedicated chapters.

Identification of Impacts, Risks and Opportunities (IROs)

Initially, Bitdefender conducted an analysis of its activities, business relationships, value chain, and affected stakeholders to pinpoint relevant sustainability matters, guided by the list specified in ESRS 1, paragraph AR16. This assessment also included a benchmark analysis relevant to Bitdefender's industry, offering a sector-specific outlook and facilitating the potential inclusion of entity-specific topics.

In line with ESRS standards, the identification and engagement of stakeholders serves as a fundamental component of the materiality assessment process. Leveraging the list of sustainability matters defined in ESRS 1 AR16, each sustainability sub-topic was assigned an Impact, Risk, and Opportunity (IRO) Manager. The IRO Managers were tasked with providing insights into sustainability matters and identifying and evaluating IROs. Each sustainability matter underwent a thorough review via interviews or workshops with the assigned IRO Manager and other internal stakeholders, focusing on pinpointing IROs at the sub-subtopic level. During August and September 2024, a total of 19 interviews were conducted, resulting in an extensive list of IROs that were subsequently assessed and prioritized according to ESRS 1 recommendations.

To inform the due diligence process in identifying IROs, Bitdefender's comprehensive risk management framework, which also tracks ESG risks, was utilized throughout.

Stakeholder engagement

The internal stakeholders consulted in the identification and evaluation process of the material sustainability matters were representatives of the following departments:

- Administration, Purchasing & Logistics
- Global Customer Engagement
- Office Management
- External Reporting
- Finance
- Business Applications
- IT Governance
- IT Operations
- Fraud Prevention and Office Security
- HSE
- Information Security
- Human Resources
- I&T and Consumer Product Delivery
- Legal Affairs
- Corporate Communications
- Product Engineering
- Product Management (Business and Consumer Groups)
- Security, Compliance and Engineering Operations
- Product & Engineering
- Sales & Marketing
- Demand Generation, eCommerce, and Partner Marketing
- Global Sales & Channels
- Cyber Threat Intelligence Lab

Bitdefender's recognizes the importance of consulting with external affected stakeholders, to understand how they may be impacted. For the 2023 Sustainability Report, Bitdefender has conducted a comprehensive stakeholder analysis to identify and prioritize key groups that have a vested interest in or are impacted by its operations. During the consultations, the opinions, concerns, and suggestions from various stakeholder groups were reviewed. For this reason, the company did not undertake another external stakeholder engagement process for the 2024 Sustainability Report. For more information regarding the engagement and the stakeholders involved in the consultation process, please see Bitdefender Group's Sustainability Report For 2023.

Assessing impact materiality

The assessment included 4 criteria for identifying and classifying impact, namely the type of impact (Actual or Potential), the nature of the impact (Positive or Negative), the time horizon in which the impact will materialize (Short, Medium or Long-term), and the location of the impact in the value chain (Upstream, Downstream, Own operations or Across the value chain).

The scoring of impacts was based on the criteria defined by the ESRS 1: severity (scale, scope and irremediability) and likelihood.

Table 6 - Impact materiality assessment criteria

Likelihood	Severity		
	Scale	Scope	Irremediability
Measures the likelihood of an impact to occur/materialize	Measures the magnitude of the impact, in terms of severity for negative impacts or in terms of how beneficial the positive impacts are.	Measures the size of negative or positive effects on the environment, society or the economy.[1]	Measures whether and to what extent negative impacts could be remediated.[2]

All these criteria form the impact materiality. The materiality score is the result of multiplying the likelihood score by the severity score, consisting of scale, scope and irremediability (in the case of negative impacts). The severity score is given by choosing the maximum score from the 2 or 3 criteria, depending on the character of the impact.

Assessing financial materiality

For financial materiality**,** the risks and opportunities were classified by two criteria: the time horizon in which the risk or opportunity is expected (Short, Medium or Long-term), and the location of the risk or opportunity in the value chain (Upstream, Downstream, Own operations or Across the value chain). The scoring of risks and opportunities was based on the criteria defined by the ESRS: magnitude and likelihood. The significance score is the result of multiplying the likelihood score by the magnitude score.

Table 7 - Financial materiality assessment criteria

Likelihood	Magnitude
Measures the likelihood of a risk or opportunity to occur/materialize.	Measures the magnitude of the financial effect a risk or opportunity would have if it were to materialize.

[1] Size refers to how widespread the impact is or how many stakeholders it impacts.
[2] Only scored for negative impacts. For positive impacts, the severity score is only based on Scale and Scope.

Thresholds

To assess the materiality of impacts, risks, and opportunities (IROs) and identify relevant sustainability matters for reporting, the company applies defined significance thresholds. In this year's analysis, IROs scoring 8 or above on the 1-16 scale were deemed material. This midpoint threshold ensures focus on issues of moderate to high significance, where the likelihood, magnitude, or scope warrants strategic attention. Scores of 1-7 typically reflect low-probability, low-impact, or localized issues that do not require immediate intervention. By applying this threshold, the company prioritizes IROs with a clear and tangible influence on operations, financial performance, or stakeholder relationships.

Results of the materiality assessment

During the Double Materiality Assessment (DMA), a total of 178 Impacts, Risks and Opportunities (IRO) topics were identified and evaluated: 70 impacts, 69 risks, and 39 opportunities. Following the assessment, 61 topics were considered material, comprising 48 impacts, 2 risks, and 10 opportunities.

The relatively low number of risks classified as material (2 out of 69) reflects the company's risk profile and its robust approach to risk management. Many of the potential risks identified during the DMA are already being effectively monitored and mitigated through existing internal processes, policies, and controls. This proactive management approach reduces the likelihood and potential significance of these risks, which in turn lowers their materiality within the DMA framework.

The company remains committed to continuously reassessing risks through future DMAs, ensuring that emerging risks are captured, monitored, and, where relevant, reclassified as material in line with evolving internal and external circumstances.

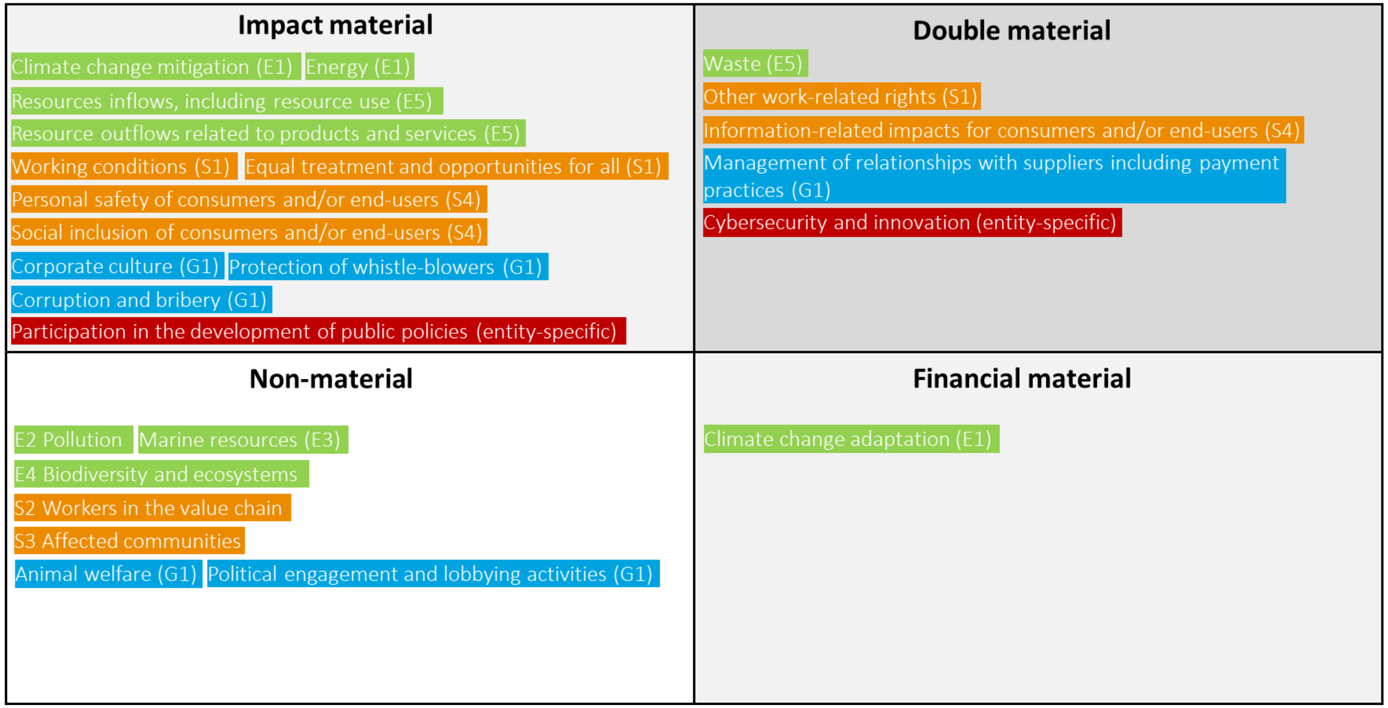
The IROs were consolidated and mapped to the list of sustainability topics described in ESRS 1 AR 16. As a result of the assessment, Bitdefender has identified 7 material topics:

- ↳ Climate change (ESRS E1)
- ↳ Circular economy (ESRS E5)
- ↳ Own workforce (ESRS S1)
- ↳ Consumers and end-users (ESRS S4)
- ↳ Business conduct (ESRS G1)
- ↳ Cybersecurity and Innovation (entity-specific)
- ↳ Participation in the development of public policies (entity-specific)

The DMA conducted for this Sustainability Statement is an integral part of our commitment to transparency and responsible business practices. While we strive to identify and address material impacts, risks, and opportunities as comprehensively as possible, the dynamic nature of sustainability issues means that there will always be room for improvement. We recognize that the methodologies and thresholds used in this assessment are based on the best available data and current understanding, but they are continuously evolving. As new information and insights become available, we will refine and enhance our processes to better capture the complexities of sustainability and its implications for our business and stakeholders.

At the sub-topic level, 19 sub-topics were identified as material:

Bitdefender’s 2 X 2 Materiality Matrix



Impact material Climate change mitigation (E1) Energy (E1) Resources inflows, including resource use (E5) Resource outflows related to products and services (E5) Working conditions (S1) Equal treatment and opportunities for all (S1) Personal safety of consumers and/or end-users (S4) Social inclusion of consumers and/or end-users (S4) Corporate culture (G1) Protection of whistle-blowers (G1) Corruption and bribery (G1) Participation in the development of public policies (entity-specific)	**Double material** Waste (E5) Other work-related rights (S1) Information-related impacts for consumers and/or end-users (S4) Management of relationships with suppliers including payment practices (G1) Cybersecurity and innovation (entity-specific)
Non-material E2 Pollution Marine resources (E3) E4 Biodiversity and ecosystems S2 Workers in the value chain S3 Affected communities Animal welfare (G1) Political engagement and lobbying activities (G1)	**Financial material** Climate change adaptation (E1)

The material impacts, risks and opportunities identified during the materiality assessment are described below, including a description of the time-horizon and of the value chain location where the material impacts, risks and opportunities are concentrated.

Table 8 - List of material impacts

Topic	Sub-topic	Sub-subtopic	Material impact	Type	Nature	Time-horizon	Location in the value chain
Climate change	Climate change mitigation	Greenhouse gas emissions (Scope 1, 2 and 3)	Operating and cooling data centers is energy-intensive. When this energy is sourced from non-renewable sources, it leads to significant indirect greenhouse gas (GHG) emissions (Scope 3)	Actual	Negative	Short-term	Across the value chain
Climate change	Climate change mitigation	Greenhouse gas emissions (Scope 1, 2 and 3)	Indirect GHG emissions generated by employee business travel, including air, road, and other modes of transportation	Actual	Negative	Short-term	Downstream
Climate change	Climate change mitigation	Greenhouse gas emissions (Scope 1, 2 and 3)	Through the design of software solutions that optimize the energy efficiency of electronic products, Bitdefender helps lower greenhouse gas (GHG) emissions associated with their operation	Actual	Positive	Short-term	Downstream
Climate change	Energy	Energy consumption and mix (renewable vs. non-renewable)	The operation of data centers requires substantial amounts of energy, which can lead to considerable environmental impacts	Actual	Negative	Short-term	Across the value chain
Climate change	Energy	Energy efficiency measures and results	Implementation of energy efficiency measures in office buildings in Romania contributes to reduced energy consumption and associated environmental impacts.	Actual	Positive	Short-term	Own operations
Circular economy	Resources inflows, including resource use	-	The fully digital enterprise division minimizes the use of physical resources, contributing to greater efficiency and reduced environmental impact	Potential	Positive	Short-term	Own operations
Circular economy	Resource outflows related to products and services	-	Bitdefender's solutions enhance the longevity of electronic products by ensuring their cybersecurity, thereby reducing the need for frequent replacements and updates.	Actual	Positive	Short-term	Own operations

Topic	Sub-topic	Sub-subtopic	Material impact	Type	Nature	Time-horizon	Location in the value chain
Circular economy	Waste	-	Operational activities generate non-hazardous waste, primarily from office use (paper, plastics, office supplies) and from packaging associated with hardware and software distribution	Actual	Negative	Short-term	Own operations
Circular economy	Waste	-	Group-wide digitalization and remote working practices, such as adopting digital-only contracts and discouraging unnecessary printing, have significantly reduced office waste generation.	Actual	Positive	Short-term	Own operations
Circular economy	Waste	-	Generation of waste from electrical and electronic equipment from decommissioned company-owned equipment (electronic equipment used by employees, office equipment and server rooms).	Actual	Negative	Short-term	Own operations
Circular economy	Waste	-	Office spaces in France have implemented a ban on plastic bottles, reducing single-use plastic consumption	Actual	Positive	Short-term	Own operations
Own workforce	Working conditions	Working time	Cyber security requirements and the need to quickly respond to security incidents may result in frequent overtime and after-hours work (for technical, security, IT operations teams)	Actual	Negative	Short-term	Own operations
Own workforce	Working conditions	Working time	Global collaboration may require meetings and communications outside of normal business hours, affecting employees' daily routines. (applicable for technical support teams)	Actual	Negative	Short-term	Own operations
Own workforce	Working conditions	Adequate wages	High demand for cybersecurity professionals prompts Bitdefender to offer competitive salaries and benefits to attract and retain top talent	Actual	Positive	Short-term	Own operations

Topic	Sub-topic	Sub-subtopic	Material impact	Type	Nature	Time-horizon	Location in the value chain
Own workforce	Working conditions	Adequate wages	The company maintains a strong wage policy, offering salary packages that comply with EU, national, and local standards on adequate, fair, and minimum wages. These packages include competitive base salaries, performance-based bonuses, and comprehensive benefits.	Actual	Positive	Short-term	Own operations
Own workforce	Working conditions	Work-life balance	Telecommuting and flexible work schedules, giving employees the flexibility to work from home and better manage their personal time	Actual	Positive	Short-term	Own operations
Own workforce	Working conditions	Work-life balance	Promoting a healthy organizational culture by offering wellness programs, mental health support, and supporting work-leisure balance can improve employee satisfaction and productivity	Actual	Positive	Short-term	Own operations
Own workforce	Working conditions	Work-life balance	Bitdefender provides family-related leave (include maternity leave, paternity leave, parental leave, and carers' leave)	Actual	Positive	Short-term	Own operations
Own workforce	Working conditions	Health and safety	To address the challenges of remote working, the company has introduced a range of health and well-being initiatives, including stress management and ergonomic training, budgets for ergonomic chairs, psychological well-being programs, and access to sports and social activities.	Actual	Positive	Short-term	Own operations
Own workforce	Equal treatment and opportunities for all	Training and skills development	The company provides comprehensive training and skills development opportunities, covering both technical and soft skills, designed to support all employees and personalized according to job requirements	Actual	Positive	Short-term	Own operations

Topic	Sub-topic	Sub-subtopic	Material impact	Type	Nature	Time-horizon	Location in the value chain
Own workforce	Equal treatment and opportunities for all	Employment and inclusion of persons with disabilities	Bitdefender fosters an inclusive workplace by employing people with disabilities and ensuring that no exclusionary criteria are applied in recruitment or employment practices	Actual	Positive	Short-term	Own operations
Own workforce	Equal treatment and opportunities for all	Measures against violence and harassment in the workplace	Mandatory trainings and procedures on workplace harassment and violence are provided during onboarding and annually, supported by regular reporting, an employee handbook, and a Code of Conduct	Actual	Positive	Short-term	Own operations
Own workforce	Other work-related rights	Privacy	Bitdefender implements advanced security solutions to protect employee data against unauthorized access and cyber attacks	Actual	Positive	Short-term	Own operations
Own workforce	Other work-related rights	Privacy	Adoption of strict privacy and security policies, which ensures that employees' personal data is managed responsibly and securely	Actual	Positive	Short-term	Own operations
Own workforce	Other work-related rights	Privacy	Data security and privacy training programs can educate employees about protecting their own data and the importance of following privacy policies	Actual	Positive	Short-term	Own operations
Consumers and end-users	Information-related impacts for consumers and/or end-users	Privacy	To safeguard user privacy, Bitdefender has implemented an End User Anonymization Policy and established a dedicated department to ensure full GDPR compliance.	Actual	Positive	Short-term	Downstream
Consumers and end-users	Information-related impacts for consumers and/or end-users	Privacy	Ensuring user security through cybersecurity products (versus third-parties), including scam prevention	Actual	Positive	Short-term	Downstream

Topic	Sub-topic	Sub-subtopic	Material impact	Type	Nature	Time-horizon	Location in the value chain
Consumers and end-users	Information-related impacts for consumers and/or end-users	Privacy	Bitdefender ensures the protection of B2B customer information through strict access controls and the exclusive use of tools that comply with the company's privacy policy and are approved by the information security team.	Actual	Positive	Short-term	Downstream
Consumers and end-users	Information-related impacts for consumers and/or end-users	Freedom of expression	Bitdefender fosters strong customer relationships by offering dedicated B2B and B2C support services, engaging openly through social media channels, and leveraging monitoring tools (e.g., Social Sprout) to respond proactively to customer needs.	Actual	Positive	Short-term	Downstream
Consumers and end-users	Information-related impacts for consumers and/or end-users	Access to (quality) information	By providing VPN solutions, Bitdefender helps customers access information safely and reliably, protecting their privacy and data security	Actual	Positive	Short-term	Downstream
Consumers and end-users	Information-related impacts for consumers and/or end-users	Access to (quality) information	Bitdefender's customers receive continuous access to information and updates about their subscriptions, along with non-commercial communications on security breaches and protection activities	Actual	Positive	Short-term	Downstream
Consumers and end-users	Information-related impacts for consumers and/or end-users	Access to (quality) information	Bitdefender enhances customer security and satisfaction by providing timely reports and information, effectively managing detection and response through its cybersecurity solutions, and delivering dedicated customer success management for the B2B segment	Actual	Positive	Short-term	Downstream
Consumers and end-users	Personal safety of consumers and/or end-users	Protection of children	Bitdefender provides parental control solutions that protect minors from harmful online content and offer reporting mechanisms to support safe digital use	Actual	Positive	Short-term	Downstream

Topic	Sub-topic	Sub-subtopic	Material impact	Type	Nature	Time-horizon	Location in the value chain
Consumers and end-users	Social inclusion of consumers and/or end-users	Access to products and services	Bitdefender implements technological support programs for start-ups, students and NGOs, while facilitating access to cybersecurity business solutions at a discounted price	Actual	Positive	Short-term	Downstream
Business conduct	Corporate culture	-	Through its global culture, Bitdefender promotes inclusion and equal opportunities, with a strong focus on advancing women in technology	Potential	Positive	Medium-term	Own operations
Business conduct	Protection of whistle-blowers	-	Whistleblowing channels for business partners are implemented and used, which has determined increased confidence from partners.	Actual	Positive	Short-term	Across the value chain
Business conduct	Protection of whistle-blowers	-	Whistleblowing channel for employees in which their anonymity is protected	Actual	Positive	Short-term	Own operations
Business conduct	Management of relationships with suppliers including payment practices	-	The lack of a group-level procurement procedure may lead to inconsistencies in supplier management and reduced oversight across the organization	Actual	Negative	Medium-term	Across the value chain
Business conduct	Corruption and bribery	Prevention and detection including training	Implementation of anti-corruption policies and procedures, including a gifting policy applicable to all business relationships, with clear consequences for violations	Actual	Positive	Medium-term	Own operations
Business conduct	Corruption and bribery	Prevention and detection including training	Bitdefender has established reporting and monitoring systems to detect, prevent, and address corruption and bribery risks	Actual	Positive	Short-term	Own operations

Topic	Sub-topic	Sub-subtopic	Material impact	Type	Nature	Time-horizon	Location in the value chain
Business conduct	Corruption and bribery	Prevention and detection including training	Employees receive dedicated training on corruption and bribery to strengthen awareness and ensure compliance with ethical business standards	Actual	Positive	Short-term	Own operations
Cybersecurity and Innovation (entity-specific)	-	-	Bitdefender helps clients strengthen their defenses by identifying breaches and shortcomings in their security systems.	Actual	Positive	Short-term	Downstream
Cybersecurity and Innovation (entity-specific)	-	-	Bitdefender operates an ethical hacking program to proactively identify vulnerabilities and strengthen cybersecurity defenses	Actual	Positive	Short-term	Own operations
Cybersecurity and Innovation (entity-specific)	-	-	Bitdefender supports the fight against cybercrime through a dedicated team that collaborates free of charge with law enforcement agencies, helping to improve their expertise and strengthen global cybersecurity resilience.	Actual	Positive	Short-term	Downstream
Cybersecurity and Innovation (entity-specific)	-	-	Free decryption program available to users	Actual	Positive	Short-term	Downstream
Cybersecurity and Innovation (entity-specific)	-	-	Minimizing security-related impacts on communities or participating in company-community partnerships. For example, free cybersecurity services are offered for hospitals and medical centers in Romania and UK	Actual	Positive	Short-term	Across the value chain

Topic	Sub-topic	Sub-subtopic	Material impact	Type	Nature	Time-horizon	Location in the value chain
Cybersecurity and Innovation (entity-specific)	-	-	The company is driving innovation in cybersecurity solutions, while also enabling safe innovation for other technologies	Actual	Positive	Short-term	Own operations
Participation in the development of public policies (entity-specific)	-	-	Contributing to cyber-resilience development for countries and citizens	Actual	Positive	Short-term	Across the value chain

Table 9 - List of material risks and opportunities

Topic	Sub-topic	Sub-subtopic	Material Risk / Opportunity	Time-horizon	Location in the value chain
Climate change	Climate change adaptation	Impact of physical climate risks on operations	Opportunity: Development and implementation of business continuity plans that include emergency measures for extreme weather events.	Short-term	Own operations
Circular economy	Waste	-	Opportunity: Implementing robust recycling programs for office supplies can reduce environmental impact and recover valuable materials.	Short-term	Own operations
Circular economy	Waste	-	Opportunity: Banning the usage of PET bottles in all Bitdefender offices	Short-term	Own operations
Own workforce	Other work-related rights	Privacy	Opportunity: Implementation of advanced technologies and strict security practices to protect employee data, which can increase employee trust and loyalty.	Short-term	Own operations

Topic	Sub-topic	Sub-subtopic	Material Risk / Opportunity	Time-horizon	Location in the value chain
Consumers and end-users	Information-related impacts for consumers and/or end-users	Privacy	Risk: Privacy breaches, mishandling or unauthorized access to customer data can determine reputational, financial and market risks	Medium-term	Across the value chain
Consumers and end-users	Information-related impacts for consumers and/or end-users	Privacy	Risk: AI implementation determines the change of business processes and operations (market risk)	Short-term	Own operations
Consumers and end-users	Information-related impacts for consumers and/or end-users	Privacy	Opportunity: Evaluations by independent institutions can enhance customer trust and differentiation (reputation, market share)	Short-term	Own operations
Business conduct	Management of relationships with suppliers including payment practices	-	Opportunity: Developing an ESG supplier assessment and procurement policy	Short-term	Own operations
Cybersecurity and Innovation (entity-specific)	-	-	Opportunity: Leveraging Bitdefender’s role in building a secure digital ecosystem as a strategic opportunity to expand market reach and customer trust.	Medium-term	Own operations
Cybersecurity and Innovation (entity-specific)	-	-	Opportunity: Being an early adopter of new technologies can generate a competitive advantage	Short-term	Own operations

Topic	Sub-topic	Sub-subtopic	Material Risk / Opportunity	Time-horizon	Location in the value chain
Cybersecurity and Innovation (entity-specific)	-	-	Opportunity: Workstream efficiency through implementation of new technologies (automation, AI)	Medium-term	Own operations
Cybersecurity and Innovation (entity-specific)	-	-	Opportunity: Through its innovation culture, Bitdefender can be more attractive to a skilled workforce	Medium-term	Own operations

E1 Disclosure requirement related to ESRS 2 IRO-1 - Description of the processes to identify and assess material climate-related impacts, risks and opportunities

The company systematically screened its operations and relevant parts of its value chain to identify climate-related impacts, risks and opportunities. The assessment included a review of the company's GHG emission sources and related dependencies, with particular attention to data center operations given their significant contribution to overall energy consumption and associated indirect emissions.

The screening confirmed that Bitdefender's most significant climate-related impact arises from the high energy demand of third-party's data centers for computing and cooling, which can materially increase indirect emissions when electricity is sourced from non-renewable energy.

This underlines both risks and opportunities, including the need to improve energy efficiency, deploy advanced cooling technologies and increase the share of renewable energy in the supply mix. While the company has not yet undertaken a formal climate scenario analysis to assess physical and transition risks over short-, medium- and long-term horizons, the screening process relied on internal expertise, sector knowledge and publicly available data to form its current understanding.

Consequently, no scenario-based modelling has yet been incorporated into the company's risk assessment or financial assumptions, though the results of the DMA provide a structured basis for future scenario work and targeted decarbonization initiatives.

E5 Disclosure Requirement related to ESRS 2 IRO-1 - Description of the processes to identify and assess material resource use and circular economy-related impacts, risks and opportunities

The company conducted a Double Materiality Assessment which entailed a systematic screening of its assets and activities to identify actual and potential impacts, risks and opportunities (IROs) related to resource inflows, resource outflows and waste across its own operations and relevant parts of the value chain. The process was implemented with the active involvement of internal stakeholders from Product Engineering, Business Sales & Channels, and Consumer Sales & Marketing, ensuring that the assessment reflected operational realities and business model characteristics.

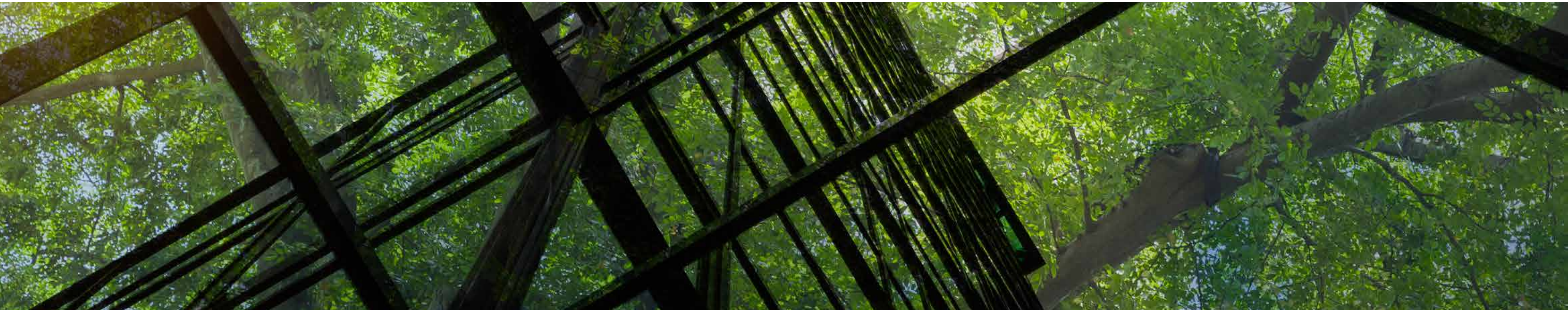
The methodology applied was aligned with the double materiality principle, capturing both impact materiality (environmental and social significance) and financial materiality (risks and opportunities for the company). IROs were assessed and prioritized using a scoring approach presented in this chapter, supported by IRO mapping matrices and structured stakeholder feedback consolidation.

The screening confirmed several relevant topics: a potential positive impact from the fully digital enterprise division in reducing physical resource use; a positive contribution from cybersecurity solutions that extend product longevity; negative impacts from office, packaging and decommissioned electronic equipment waste; and positive impacts from digitalisation initiatives and bans on single-use plastics. Additional opportunities were identified in enhancing recycling programmes and recovering PET bottles to reduce environmental impacts and improve resource efficiency.

G1 Disclosure Requirement related to ESRS 2 IRO-1 - Description of the processes to identify and assess material impacts, risks and opportunities

Bitdefender screened its operations and value chain to identify impacts, risks and opportunities related to business conduct, focusing on the code of conduct, anti-corruption, whistleblower protection and supplier management. The process involved key internal functions including Compliance, Legal Affairs, Fraud Prevention and Purchasing.

This confirmed positive impacts from whistleblowing channels for employees and partners, a strong culture of inclusion and equal opportunities, and the implementation of anti-corruption measures such as policies, monitoring systems and employee training. A negative impact was identified in the absence of a group-level procurement procedure, while an opportunity was recognized in developing an ESG supplier assessment and procurement policy. These findings provide a structured basis for strengthening governance practices and ensuring responsible business conduct across operations and the value chain.



Disclosure Requirement IRO-2 - Disclosure Requirements in ESRS covered by the undertaking's sustainability statement

Table 10 - Disclosure Requirements in ESRS covered by Bitdefender's sustainability statement

Disclosure Requirement	Location in the Sustainability Statement (page)
Basis for preparation	
Disclosure Requirement BP-1 - General basis for preparation of sustainability statements	5
Disclosure Requirement BP-2 - Disclosures in relation to specific circumstances	7
Governance	
Disclosure Requirement GOV-1 - The role of the administrative, management and supervisory bodies	10
Disclosure Requirement GOV-2 - Information provided to and sustainability matters addressed by the undertaking's administrative, management and supervisory bodies	13
Disclosure Requirement GOV-3 - Integration of sustainability-related performance in incentive schemes	13
Disclosure Requirement GOV-4 - Statement on due diligence	13
Disclosure Requirement GOV-5 - Risk management and internal controls over sustainability reporting	14
Strategy	
Disclosure Requirement SBM-1 - Strategy, business model and value chain	16
Disclosure Requirement SBM-2 - Interests and views of stakeholders	23
Disclosure Requirement SBM-3 - Material impacts, risks and opportunities and their interaction with strategy and business model	24
Impact, risk and opportunity management	
Disclosure Requirement IRO-1 - Description of the processes to identify and assess material impacts, risks and opportunities	24

Disclosure Requirement	Location in the Sustainability Statement (page)
Disclosure Requirement IRO-2 - Disclosure requirements in ESRS covered by the undertaking's sustainability statement	41
ESRS E1 - Climate change	
Governance	
Disclosure requirement related to ESRS 2 GOV-3 - Integration of sustainability-related performance in incentive schemes	13
Strategy	
Disclosure Requirement E1-1 - Transition plan for climate change mitigation	48
Disclosure Requirement related to ESRS 2 SBM-3 - Material impacts, risks and opportunities and their interaction with strategy and business model	64
Impact, risk and opportunity management	
Disclosure requirement related to ESRS 2 IRO-1 - Description of the processes to identify and assess material climate-related impacts, risks and opportunities	39
Disclosure Requirement E1-2 - Policies related to climate change mitigation and adaptation	49
Disclosure Requirement E1-3 - Actions and resources in relation to climate change policies	51
Metrics and targets	
Disclosure Requirement E1-4 - Targets related to climate change mitigation and adaptation	51
Disclosure Requirement E1-5 - Energy consumption and mix	51
Disclosure Requirement E1-6 - Gross Scopes 1, 2, 3 and Total GHG emissions	53
Disclosure Requirement E1-7 - GHG removals and GHG mitigation projects financed through carbon credits	Not material
Disclosure Requirement E1-8 - Internal carbon pricing	Not material

Disclosure Requirement	Location in the Sustainability Statement (page)
Disclosure Requirement E1-9 - Anticipated financial effects from material physical and transition risks and potential climate-related opportunities	Use of exemption for disclosure
ESRS E5 - Resource use and circular economy	
Impact, risk and opportunity management	
Disclosure Requirement related to ESRS 2 IRO-1 - Description of the processes to identify and assess material resource use and circular economy-related impacts, risks and opportunities	40
Disclosure Requirement E5-1 - Policies related to resource use and circular economy	55
Disclosure Requirement E5-2 - Actions and resources related to resource use and circular economy	55
Metrics and targets	
Disclosure Requirement E5-3 - Targets related to resource use and circular economy	56
Disclosure Requirement E5-4 - Resource inflows	56
Disclosure Requirement E5-5 - Resource outflows	57
Disclosure Requirement E5-6 - Anticipated financial effects from resource use and circular economy-related impacts, risks and opportunities	Use of exemption for disclosure
ESRS S1 - Own workforce	
Strategy	
Disclosure Requirement related to ESRS 2 SBM-2 - Interests and views of stakeholders	64
Disclosure Requirement related to ESRS 2 SBM-3 - Material impacts, risks and opportunities and their interaction with strategy and business model	64
Impact, risk and opportunity management	
Disclosure Requirement S1-1 - Policies related to own workforce	66

Disclosure Requirement	Location in the Sustainability Statement (page)
Disclosure Requirement S1-2 - Processes for engaging with own workers and workers' representatives about impacts	69
Disclosure Requirement S1-3 - Processes to remediate negative impacts and channels for own workers to raise concerns	70
Disclosure Requirement S1-4 - Taking action on material impacts on own workforce, and approaches to mitigating material risks and pursuing material opportunities related to own workforce, and effectiveness of those actions	73
Metrics and targets	
Disclosure Requirement S1-5 - Targets related to managing material negative impacts, advancing positive impacts, and managing material risks and opportunities	75
Disclosure Requirement S1-6 - Characteristics of the undertaking's employees	76
Disclosure Requirement S1-7 - Characteristics of non-employee workers in the undertaking's own workforce	81
Disclosure Requirement S1-8 - Collective bargaining coverage and social dialogue	Not material
Disclosure Requirement S1-9 - Diversity metrics	82
Disclosure Requirement S1-10 - Adequate wages	83
Disclosure Requirement S1-11 - Social protection	Not material
Disclosure Requirement S1-12- Persons with disabilities	83
Disclosure Requirement S1-13 - Training and skills development metrics	84
Disclosure Requirement S1-14 - Health and safety metrics	86
Disclosure Requirement S1-15 - Work-life balance metrics	86
Disclosure Requirement S1-16 - Compensation metrics (pay gap and total compensation)	87
Disclosure Requirement S1-17 - Incidents, complaints and severe human rights impacts	87

Disclosure Requirement ESRS S4 - Consumers and end-users	Location in the Sustainability Statement (page)
Strategy	
Disclosure Requirement related to ESRS 2 SBM-2 - Interests and views of stakeholders	88
Disclosure Requirement related to ESRS 2 SBM-3 - Material impacts, risks and opportunities and their interaction with strategy and business mode	89
Impact, risk and opportunity management	
Disclosure Requirement S4-1 - Policies related to consumers and end-users	101
Disclosure Requirement S4-2 - Processes for engaging with consumers and end-users about impacts	103
Disclosure Requirement S4-3 - Processes to remediate negative impacts and channels for consumers and end-users to raise concerns	105
Disclosure Requirement S4-4 - Taking action on material impacts on consumers and end-users, and approaches to managing material risks and pursuing material opportunities related to consumers and end- users, and effectiveness of those actions	107
Metrics and targets	
Disclosure Requirement S4-5 - Targets related to managing material negative impacts, advancing positive impacts, and managing material risks and opportunities	112
ESRS G1 - Business conduct	
Governance	
Disclosure Requirement related to ESRS 2 GOV-1 - The role of the administrative, supervisory and management bodies	114
Impact, risk and opportunity management	
Disclosure Requirement related to ESRS 2 IRO-1 - Description of the processes to identify and assess material impacts, risks and opportunities	24
Disclosure Requirement G1-1– Business conduct policies and corporate culture	114
Disclosure Requirement G1-2 - Management of relationships with suppliers	117
Disclosure Requirement G1-3 - Prevention and detection of corruption and bribery	118

Disclosure Requirement	Location in the Sustainability Statement (page)
Metrics and targets	
Disclosure Requirement G1-4 - Confirmed incidents of corruption or bribery	119
Disclosure Requirement G1-5 - Political influence and lobbying activities	119
Disclosure Requirement G1-6 - Payment practices	120

Safeguarding the Environment

Bitdefender is deeply committed to environmental sustainability, recognizing that our responsibility extends beyond digital security to include protecting the planet. We understand that in today’s business environment, leading in cybersecurity also means leading in sustainable practices. To this end, we are in the process of developing an a forward-thinking Environmental, Social, and Governance (ESG) strategy that reflects our dedication to both regulatory excellence and proactive environmental stewardship.

In this chapter:

ESRS E1 Climate change

Strategy

Disclosure Requirement E1-1 - Transition plan for climate change mitigation

Bitdefender is currently in the process of developing its Environmental, Social, and Governance (ESG) reporting framework in accordance with the European Sustainability Reporting Standards (ESRS) and the Corporate Sustainability Reporting Directive (CSRD). As part of this ongoing effort, the company is focused on establishing a solid foundation for reporting sustainability metrics, which includes collecting the necessary data and calculating its greenhouse gas (GHG) emissions.

Due to this focus, Bitdefender does not yet have a transition plan in place for climate change mitigation for the year 2024. The transition plan is a critical component of our developing sustainability strategy, and we intend to develop and implement it once we have fully gathered the relevant data on our environmental impact. This will enable us to set clear and actionable targets for reducing emissions and improving our environmental performance.

We anticipate that the transition plan will be finalized and operational no later than 2026, following the completion of data collection, GHG emissions calculation, and the establishment of a comprehensive reporting framework. Until that time, our priority remains ensuring that we meet the reporting and disclosure requirements outlined by the ESRS and CSRD, which will serve as the basis for our future sustainability strategy.

Disclosure Requirement related to ESRS 2 SBM-3 - Material impacts, risks and opportunities and their interaction with strategy and business model

As part of the Double Materiality Assessment, Bitdefender has identified several climate-related physical and transition risks. Although these risks were assessed as non-material in this sustainability statement, the company remains committed to monitoring them closely.

Bitdefender does not currently have a dedicated resilience strategy addressing climate change risks. Existing risk mitigation measures focus primarily on earthquakes, cyberattacks, and geopolitical events, while business continuity plans are tailored to these specific threats. Climate-related physical and transition risks are not yet integrated into these frameworks. Developing a comprehensive climate resilience approach will be considered as part of the company's ESG framework and the enhancement of its overall risk management in the coming years.

Table 11 - List of climate-related risks

Type of risk	Risk description
Climate-related physical risk	↳ Physical damage to infrastructure caused by extreme climate and weather events. Flooding, storms, hurricanes, wildfires can damage buildings, data centers, offices and IT equipment, disrupt power supplies, and disrupt communications, which can lead to shutdowns of operations (Particularly relevant for Bitdefender U.S.A. - Texas and Florida offices).
Climate-related transition risks	↳ Failure to comply with environmental regulations related to pollution and emissions may lead to violations of the law, fines and regulatory penalties; ↳ Failure to comply with emission standards or environmental regulations can limit market access and expansion opportunities, especially in regions with strict environmental requirements; ↳ Regulatory actions regarding environmental incidents can disrupt business operations, leading to downtime, increased costs and reputational damage; ↳ Lack of due diligence of direct and indirect suppliers, which may lead to collaboration with entities that are not aligned with Bitdefender values regarding emissions and pollution; ↳ Difficulty in meeting regulatory requirements or standards related to renewable energy use (lack of documents or reports from which the share of energy from renewable sources can be derived may determine regulatory compliance issues); ↳ Lack of data availability regarding energy consumption and mix in all Bitdefender locations (offices) may determine inefficient energy management, inaccurate reporting and difficulty in strategic planning.

Impact, risk and opportunity management

Disclosure Requirement E1-2 - Policies related to climate change mitigation and adaptation

Environmental Policy

In 2024, Bitdefender adopted an Environmental Policy outlining its commitment to responsible environmental practices and to managing energy consumption and greenhouse gas (GHG) emissions. While the current policy does not yet comprehensively address climate change adaptation, energy efficiency, or renewable energy deployment, these areas are being considered within the broader development of our ESG framework. The policy is subject to ongoing review, and additional procedures and focus areas will be incorporated over time, with new topics planned for inclusion in 2025.

As part of this Policy, the company has established a structured set of procedures for calculating its Scope 1 and Scope 2 greenhouse gas (GHG) emissions, forming a critical element of our climate change mitigation efforts. These procedures ensure accurate measurement, monitoring, and reporting of emissions, enabling us to identify reduction opportunities and track progress over time. Beyond emissions management, the Environmental Policy addresses a broad range of environmental aspects, including pollution prevention and resource conservation, waste management, hazardous substances control, energy consumption and GHG emissions, water management, and materials restrictions. Together, these measures provide a comprehensive framework for minimizing our environmental footprint and promoting responsible resource use.

This policy applies to all Bitdefender employees, contractors, and third-party partners globally. It covers all operations, including but not limited to:

Product Development: Incorporating environmental considerations into the design and development of software products and services. This includes optimizing code for energy efficiency, minimizing the environmental impact of development tools and processes, and considering the environmental footprint of software deployment and use.

- **Office Management**: Implementing sustainable practices in the management of rented office spaces.
- **Corporate Activities**: Ensuring that all business activities, including marketing, sales, and logistics, are conducted in an environmentally responsible manner.
- **Supply Chain**: Working with suppliers and partners to promote sustainability and reduce the environmental impact of the entire supply chain.
- **Green Building Initiatives**: Partnering with landlords to implement sustainable practices in rented office spaces, optimizing layouts for natural light and ventilation, using eco-friendly materials, and ensuring healthy indoor environments with proper ventilation and air quality monitoring.

Ultimate accountability for the implementation of the Environmental Policy rests with the CEO, who ensures that environmental commitments are upheld across the organization. Working closely with the Risk & Audit Committee, the CEO oversees the integration of ESG considerations into the company's corporate strategy, ensuring alignment with its mission, vision, and long-term strategic goals to foster sustainable and ethical business practices.

Executive management is responsible for embedding environmental considerations into business strategies and day-to-day operations, as well as for allocating the necessary resources to support effective policy implementation.

At the operational level, the Sustainability Project Manager and the HSE Manager (who also carries environmental responsibilities) are tasked with implementing the Environmental Policy and ensuring compliance with applicable environmental laws, regulations, and standards. They monitor environmental performance, track progress against objectives, and provide regular updates to executive management.

Through the implementation of this policy, Bitdefender commits to respect the following third-party standards and treaties:

- **ISO 14001**: Environmental Management Systems: An international standard that specifies requirements for an effective environmental management system.
- **Paris Agreement**: An international treaty on climate change, aiming to limit global warming to well below 2 degrees Celsius, preferably to 1.5 degrees Celsius, compared to pre-industrial levels.
- **Montreal Protocol**: An international treaty designed to protect the ozone layer by phasing out the production of numerous substances responsible for ozone depletion.

Disclosure Requirement E1-3 - Actions and resources in relation to climate change policies

No significant climate change mitigation or adaptation actions were identified or implemented during the reporting period. While some climate-related impacts and risks were noted - particularly those associated with greenhouse gas emissions from outsourced data centers and business travel - no specific or formalized actions have yet been defined to address these risks. This year, the company calculated its Scope 1 and Scope 2 greenhouse gas emissions, which will guide future actions and allocation of resources related to climate change.

Metrics and targets

Disclosure Requirement E1-4 - Targets related to climate change mitigation and adaptation

As of 2024, Bitdefender has not yet established formal climate-related targets. During this year, our primary focus has been on developing a robust ESG framework aligned with the requirements of the Corporate Sustainability Reporting Directive (CSRD) and the European Sustainability Reporting Standards (ESRS). We recognize the importance of setting measurable climate objectives and intend to define and commit to climate-related targets within the next two years.

Disclosure Requirement E1-5 - Energy consumption and mix

Table 12 - Energy consumption and mix

Energy consumption and mix	2024
(1) Fuel consumption from coal and coal products (MWh)	-
(2) Fuel consumption from crude oil and petroleum products (MWh)	70.99
(3) Fuel consumption from natural gas (MWh)	871.681
(4) Fuel consumption from other fossil sources (MWh)	-
(5) Consumption of purchased or acquired electricity, heat, steam, and cooling from fossil sources (MWh)	395.969
(6) Total fossil energy consumption (MWh) (calculated as the sum of lines 1 to 5)	1,333.06
Share of fossil sources in total energy consumption (%)	69.63%
(7) Consumption from nuclear sources (MWh)	190.8

Energy consumption and mix	2024
Share of consumption from nuclear sources in total energy consumption (%)	9.96%
(8) Fuel consumption for renewable sources, including biomass (also comprising industrial and municipal waste of biologic origin, biogas, renewable hydrogen, etc.) (MWh)	-
(9) Consumption of purchased or acquired electricity, heat, steam, and cooling from renewable sources (MWh)	390.389
(10) The consumption of self-generated non-fuel renewable energy (MWh)	-
(11) Total renewable energy consumption (MWh) (calculated as the sum of lines 8 to 10)	390.389
Share of renewable sources in total energy consumption (%)	20.39%
Total energy consumption (MWh) (calculated as the sum of lines 6, and 11)	**1,914.2**

Estimation methodology

In the absence of data on electricity consumption by source, an approximation method based on the national energy mix was used to estimate the proportions of electricity consumption from fossil, nuclear and renewable sources. Data on the structure of electricity production by source for each country where electricity consumption was reported was taken from the Global Electricity Generation by Source 2024 | Low-Carbon Power Data website.

This national distribution was applied proportionally to the total electricity consumption recorded in the respective country, thus obtaining an estimate from proxy data of electricity consumption, broken down by fossil, renewable and nuclear sources.

Electricity consumption from data centers

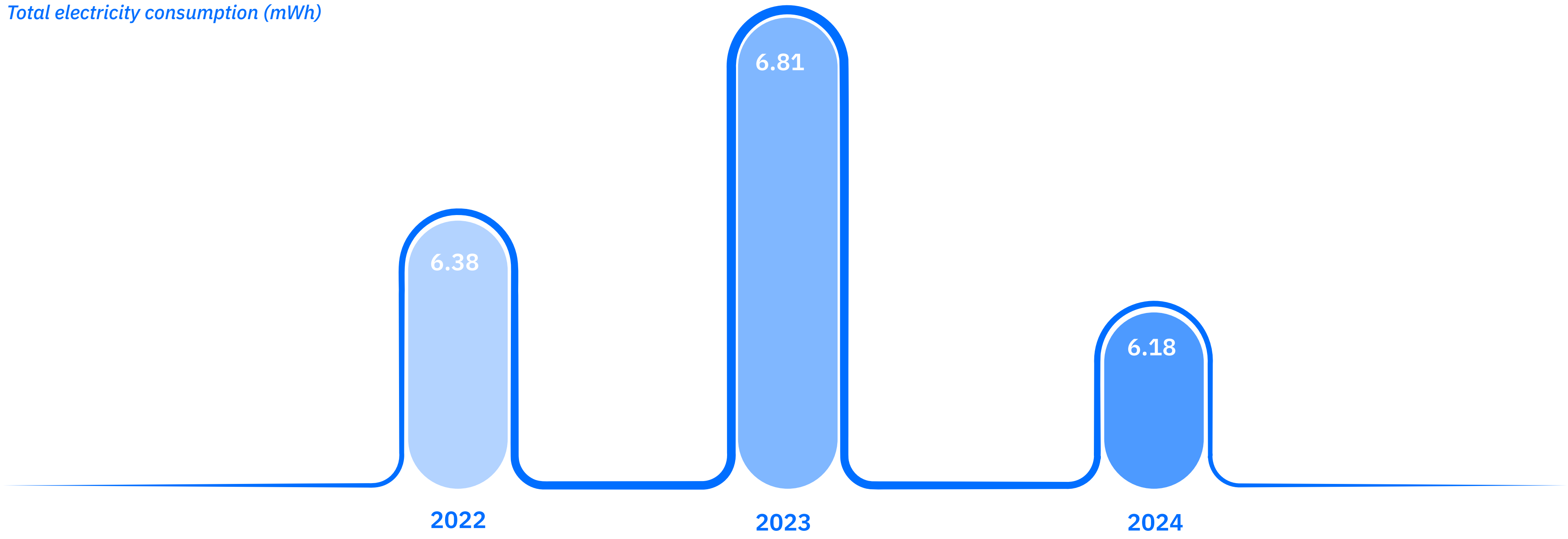
In selecting our cloud and data center providers, Bitdefender prioritizes those who actively report the carbon footprint of the services they deliver. All our data center providers utilize clean energy sources, reflecting our commitment to minimizing environmental impact. Leading providers like Google Cloud Platform (GCP), Amazon Web Services (AWS), Microsoft Azure, and Cloudflare not only offer detailed CO2 emissions reports but also participate in significant climate initiatives.

These providers are committed to “The Climate Pledge” which strives to achieve the goals of the Paris Agreement a decade early, by 2040. Furthermore, each of these companies has made substantial commitments to achieving carbon neutrality by 2030 or 2040, largely through investments in renewable energy sources such as solar and wind. This alignment with sustainability goals ensures that Bitdefender’s digital operations are supported by infrastructure that is both reliable and environmentally responsible.

Approximately three quarters of Bitdefender’s total electricity consumption is attributed to data centers, an essential element for carrying out its activities. In 2024, the electricity consumption attributed to data centers was **5,205 MWh**.

Bitdefender is choosing cloud providers and on-premises colocation data center that are using in their power supply providers that obtain energy from clean sources. All the Bitdefender datacenter providers are using a mix of fossil and clean, renewable energy.

Total electricity consumption (mWh)



Disclosure Requirement E1-6 - Gross Scope 1, 2, 3 and Total GHG emissions

Climate change is an imminent and growing challenge, reflected in the alarming trend of rising global temperatures and the intensification of extreme weather events. The scientific consensus indicates that human activities, particularly the burning of fossil fuels, are major drivers of this change. In the past decade alone, average annual temperatures have reached record levels, and the frequency and intensity of extreme weather events, such as stronger hurricanes caused by warming oceans, have increased significantly.

This reality underscores the critical need for rigorous carbon footprint calculations. By quantifying greenhouse gas emissions, Bitdefender can lay the foundation for identifying key areas for reduction, aligning strategies with climate action, and, ultimately, contributing to the global effort to mitigate the impacts of climate change.

For these reasons, 2024 marks the first year in which Bitdefender calculates its carbon footprint for Scope 1 and 2 emissions. Our GHG emissions inventory includes all relevant emission sources within the company, structured according to the GHG Protocol.

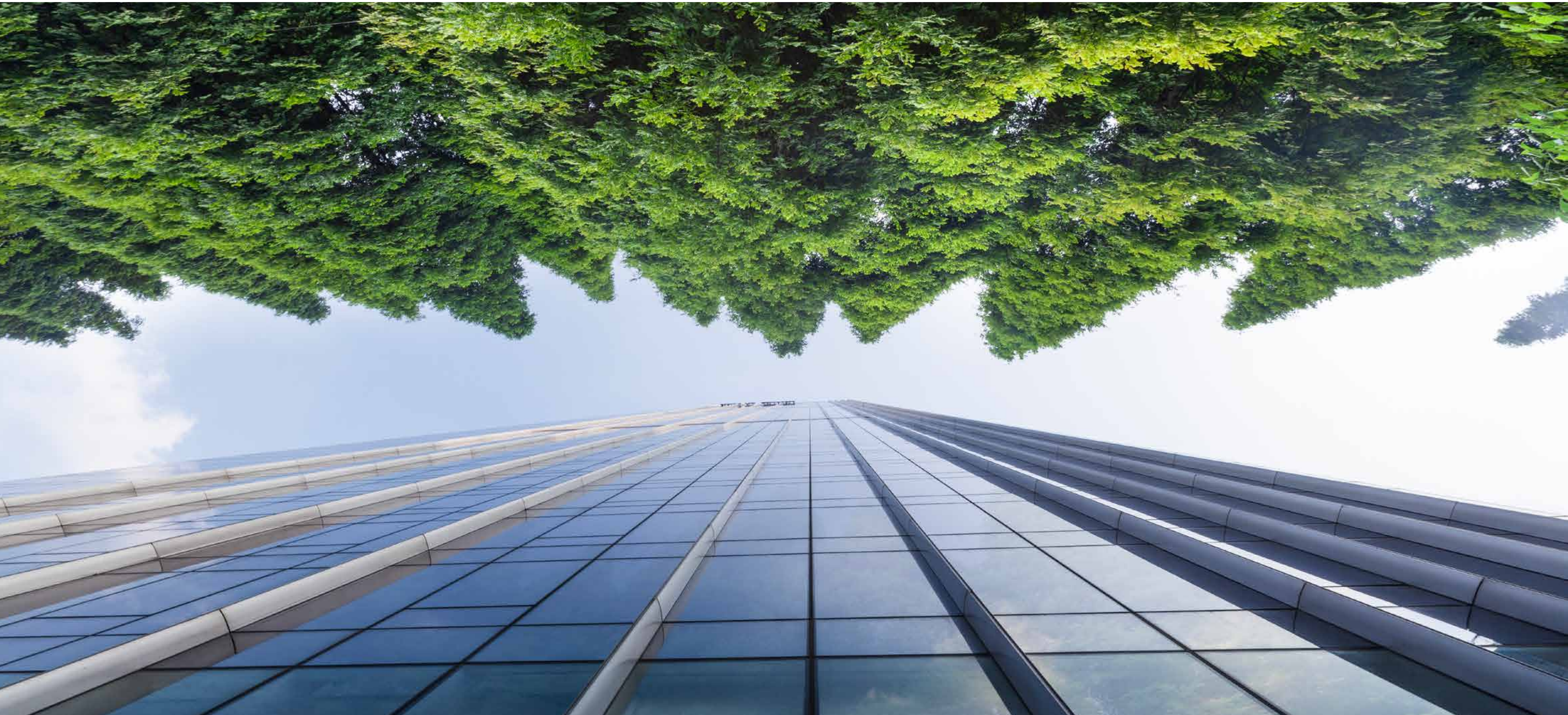
Scope 1 covers all direct emissions from sources owned or controlled by Bitdefender, including, but not limited to, company vehicles and on-site fuel combustion.

Scope 2 includes indirect emissions resulting from the production of electricity, steam, heating and cooling purchased and consumed by the company.

Table 13 - Scope 1, 2 and Total GHG Emissions (including GHG intensity to net revenue)

Scope	Amount (tCO2)	Intensity value (tCO2e/million USD)
Scope 1	194.8	0.045
Scope 2 (location based)	182.23	0.042
Total GHG Emissions (location based)	**377.06**	**0.087**

GHG intensity to net revenue is a key metric that measures Bitdefender's greenhouse gas emissions relative to its financial performance. Rather than just looking at total emissions, this metric helps assess how effectively a company is reducing its carbon footprint while generating revenue.



ESRS E5 Resource use and circular economy

Impact, risk and opportunity management

Disclosure Requirement E5-1 - Policies related to resource use and circular economy

Bitdefender has established an Environmental Policy that outlines the company's commitment to responsible resource management, waste reduction, and environmental protection across its operations. This policy provides the foundation for addressing the environmental impacts associated with our internal activities, as well as our broader value chain.

As a cybersecurity software company with both digital and limited physical product lines, we recognize the environmental impact associated with the extraction and use of virgin materials. Our environmental policy supports a gradual transition away from virgin resource use, wherever operationally feasible, and prioritizes the adoption of recycled or secondary materials across our value chain.

While our core business remains digital, we are aware of the indirect material consumption associated with server infrastructure and employee equipment. We promote responsible e-waste management and engage with vendors who refurbish or reuse components, contributing to a more circular economy. We are also actively exploring programs for extending device lifecycle through repair, reuse, and donation schemes.

Bitdefender is committed to sustainable sourcing practices and prioritizes the use of renewable resources where applicable, in alignment with our broader environmental and ethical supply chain policies. For physical product lines, including packaging and hardware accessories, we require suppliers to adhere to responsible sourcing criteria. In our digital infrastructure, while most of our operations are software-based, we work closely with data center providers and cloud partners who demonstrate environmental performance.

Bitdefender's Environmental Policy includes a commitment to minimize the environmental impact of sourced materials by encouraging innovation in low-impact alternatives.

For more information regarding the scope, accountability for implementation and references to third-party standards, legislation or initiatives please refer to Disclosure Requirement E1-2 - Policies related to climate change mitigation and adaptation.

Disclosure Requirement E5-2 - Actions and resources related to resource use and circular economy

As a software company with a hybrid operating model that combines remote and office-based work, Bitdefender's main resource consumption arises from energy and electronic equipment used by employees and for IT infrastructure, from materials needed for corporate facilities, and from packaging and hardware used in physical product distribution. Device procurement for more than 2,000 employees is managed through a centralized asset lifecycle program, ensuring both efficient use and responsible end-of-life recovery. A centralized device management system also tracks IT assets across their lifecycle, supporting refurbishment, redeployment, and donation, while decommissioned equipment is diverted from landfill and recycled through ISO 14001-certified partners.

The company is optimizing its office locations for resource efficiency, introducing waste management systems that segregate and recycle paper, plastics, and e-waste. In parallel, the shift toward cloud-based services and virtual product delivery has reduced reliance on physical media and packaging, significantly lowering material inputs per unit of product delivered.

Bitdefender's approach to circularity emphasizes extending product life, reducing material inputs, and promoting reuse and recycling. A hardware reuse program ensures that eligible devices are refurbished, donated, or responsibly recycled through certified e-waste partners. Logistics and fulfillment partners apply just-in-time practices to reduce overproduction and limit obsolete stock, thereby minimizing material waste. To support continuous improvement, internal data collection systems are being developed to better measure and report the environmental and operational impacts of reuse and lifecycle extension in future reporting cycles.

Sustainable procurement plays a central role in this strategy. Bitdefender prioritizes suppliers that provide modular and repairable devices, certified equipment such as EPEAT, TCO, and Energy Star, and access to trade-in or closed-loop recycling programs. Procurement practices are aligned with EU REACH and RoHS regulations, responsible sourcing schemes, and conflict-free mineral standards. Internal policies are designed to extend hardware use to three to four years where performance permits, thereby reducing the demand for new raw materials and supporting circular economy goals.

To advance its commitments, Bitdefender collaborates with upstream and downstream partners, local networks, and industry groups to develop initiatives that reduce material waste, promote reuse, and extend product lifecycles. In key operational regions, the company works with authorized e-waste recyclers and collection services to ensure the secure and responsible disposal of decommissioned IT and promotional hardware. Beyond operational practices, Bitdefender also engages in industry working groups on green IT, sustainable procurement, and digital product stewardship, contributing to shared knowledge and the promotion of best practices across the sector.

Metrics and targets

Disclosure Requirement E5-3 - Targets related to resource use and circular economy

At present, Bitdefender has not yet established formal targets related to resource inflows and resource outflows in the context of circular economy practices.

However, as part of our ongoing commitment to enhance sustainability performance, Bitdefender intends to define relevant targets once our ESG framework is fully developed and aligned with the Corporate Sustainability Reporting Directive (CSRD) and the European Sustainability Reporting Standards (ESRS).

Disclosure Requirement E5-4 - Resource inflows

Although our core operations focus on software development and digital services delivery, we recognize that our limited physical production and operational infrastructure still involve resource inflows that carry environmental and social implications. Our physical products are produced in small batches and typically include plastic components and associated packaging. These products are manufactured and distributed by an external partner, based on our design and technical specifications.

As the production of our physical goods is outsourced to partners who operate under environmentally responsible manufacturing standards. Our partners integrate environmentally friendly manufacturing and packaging solutions, in line with ISO 14001 standards and European Union environmental legislation, compliance with EPA environmental guidelines, signatory of The Climate Pledge, committing to reach Net Zero Carbon By 2040.

Bitdefender's infrastructure consists of offices, IT equipment, and data servers that support the delivery of global digital services. Wherever possible, we operate from energy-efficient buildings with recognized green certifications. Servers, computers, and networking equipment make up a significant share of our capital assets, and we ensure their responsible end-of-life management through certified e-waste recycling partners.

During the reporting period, the materials used in the production of our physical goods consisted primarily of plastic components. Each unit includes a small internal plastic component and an external plastic casing. At this stage, we do not have access to complete data regarding the total weight of materials used in the production of our physical products. However, we recognize the importance of this information and are committed to developing a dedicated procedure to accurately quantify and report all materials used.

No biological materials were used in the production of these goods. Although our physical material use is limited, we remain committed to responsible material sourcing, lightweight product design, and exploring sustainable alternatives for future production cycles.

Currently, Bitdefender does not calculate the weight of recycled components used to manufacture its products due to lack of data availability.

Disclosure Requirement E5-5 - Resource outflows

Products and materials

As a company operating in the technology and cybersecurity sector, Bitdefender's operations are primarily digital, with minimal physical manufacturing. Nevertheless, our business activities generate waste streams that are characteristic of the software and IT services industry, particularly from office-based operations and electronic equipment use.

The following waste streams are considered most relevant to our sector and business activities:

Table 14 - Waste streams

Waste Stream	Main Sources	Notes/Significance
Electronic Waste	Laptops, desktops, networking hardware, peripherals, toner	Critical waste stream, potential hazardous content, recycling challenges
Paper & Cardboard	Office printing, packaging, documentation	Common in office operations
Plastic Waste	Bottled water, food packaging, office consumables	Single-use plastics from daily office activities
Organic & Food Waste	Kitchen and break areas	Generated across office locations

Given our business model, we do not produce any: industrial by products, hazardous chemical waste, packaging intensive goods at scale or construction waste.

As a cybersecurity company, Bitdefender’s products are digital and designed to be cloud-based, continuously updated, and delivered electronically. This naturally supports circularity by reducing the need for physical goods and optimizing resource use over time. However, for the physical components we produce-such as plastic scratch cards, secure casings, and marketing materials-we apply circular design principles where feasible, focusing on durability, recyclability, and material efficiency.

Table 15 - Circular design characteristics of physical components

Physical components	Circular design characteristics
Plastic scratch cards	Durable design to extend lifespan (3-5 years use). Manufactured with partial recycled plastic content.
Protective plastic casing	Designed for long-term use and mechanical resilience. Modular design simplifies disassembly and recycling.
Marketing materials	Minimal ink and lamination.
Packaging components	Use of biodegradable fillers. Flat-pack and mono-material boxes for easy recycling.

Although physical products represent a small fraction of our market presence and are manufactured/distributed via third-party partners, we maintain strict oversight of quality and lifecycle standards.

- **Scratch cards**: These are engineered to provide a secure, tamper-evident layer over the activation key. While intended for one-time use, the materials used are compliant with standard industry practices in terms of print longevity, abrasion resistance, and protection against unauthorized access. Their shelf life under normal storage conditions is typically 2-3 years, which aligns with the average in the industry for prepaid access materials.
- **Plastic casings**: The casings used to house the scratch cards are made from durable, lightweight plastic, offering protection during shipping and handling. While they are not intended for long-term use, their structural integrity ensures that the activation materials inside are preserved in good condition until use. Wherever possible, we collaborate with partners that offer recyclable or low-impact materials to minimize waste.

Our physical products are designed for secure delivery of digital licenses, prioritizing security and usability over extended reuse. While conventional reparability scoring is not applicable, we continuously review material sourcing and packaging to improve sustainability without compromising product integrity.

Currently, our physical products consist mainly of scratch cards and plastic casings produced by external partners in compliance with packaging and materials regulations. Scratch cards are tamper-evident and intended for one-time use to protect activation keys, while casings are lightweight, recyclable single-component structures.

Although we do not yet calculate the share of recyclable content, we recognize the importance of transparency and material traceability in advancing circularity goals. As soon as possible we will begin:

- tracking the total weight of materials used across all physical products and packaging;
- identifying the proportion of recyclable materials, both post-industrial and post-consumer;

- ↳ working with our external partners to improve packaging sustainability, including transitioning toward recyclable, biodegradable, or reusable materials wherever feasible.
- ↳ Electronic equipment

Regarding the electronic equipment used in our operations, we apply the following principles to their procurement, use, and disposal:

Durability and repairability: devices are selected based on energy efficiency and repairability

Asset Lifecycle Tracking: all company devices are registered and tracked through an internal asset management system

Reuse and Redeployment: functional equipment is reassigned or donated internally before being considered obsolete

Certified E-waste Recycling: all discarded electronics are sent to authorized WEEE recyclers, compliant with EU Directive 2012/19/EU

Ensuring Software Longevity and Reliability

While we are not a hardware producer, our digital-first products and services are engineered with long-term viability and minimal obsolescence in mind. The software offerings demonstrate equal or superior durability compared to industry benchmarks, aligning with our broader sustainability and quality goals.

Given that the core of our business is built around digital services, primarily cybersecurity software, the concept of "product durability" takes on a different dimension compared to traditional manufacturing industries. In our context, durability is reflected in the longevity, reliability, and maintainability of both our software platforms and the limited physical products distributed through third-party partners.

Our software offerings are designed for long-term operational resilience and scalability. Key aspects include:

- ↳ **Lifecycle Support**: Core cybersecurity solutions and platforms are supported for a minimum of 5-7 years, with extended support contracts available, exceeding the average industry standard of 3-5 years.
- ↳ **Backward Compatibility and Updates**: Our products are developed with a modular architecture, allowing backward compatibility and regular security and functionality updates without requiring system replacement—this extends usable lifespans significantly beyond industry norms.
- ↳ **Cloud-Based Resilience:** A large share of our services is cloud-native, ensuring minimal system obsolescence and enabling seamless scalability as client needs evolve. This approach supports a model of continuous delivery and reduces the need for re-deployment cycles, which in turn increases overall "durability."

Waste

As a technology and cybersecurity company with operations in Europe, North America, Middle East, Australia and Asia, our business model is primarily digital. However, like any large-scale organization, our activities generate waste, primarily through office operations (paper, packaging, general consumables), IT and electronic equipment lifecycle management, and cleaning and maintenance services.

In 2024, our global office operations generated an estimated 26,000 kilograms of total waste, comprising both general office waste and electronic waste (e-waste). The majority of this waste was non-hazardous, with the exception of electronic components and printer toners, which may be classified as hazardous under applicable local and EU regulations.

Table 16 - Total waste generated in 2024 and its composition

Type of waste	Total quantity of waste generated in 2024 (kg)
Plastic	7,200
Paper and cardboard	4,800
General and organic/food waste	11,000
E-waste and toner cartridges	3,000
Total	**26,000**

As a software-driven business, the majority of the waste generated in 2024 is classified as non-hazardous, including paper, packaging materials, and general office waste. A small proportion is categorized as electronic waste, which may include items deemed hazardous under applicable local regulations.

Thanks to internal waste sorting practices and cooperation with certified recycling partners, a significant share of this waste was diverted from disposal and recycled.

- ↳ **Plastic**: Recycled through local waste streams; primarily composed of beverages bottles and packaging from office consumption;
- ↳ **Paper and cardboard**: Collected separately in all offices and sent to recycling;
- ↳ **Electronic waste and toner cartridges**: Handled through specialized e-waste recycling partners.

Plastic, paper/cardboard, e-waste and cartridges account for a combined total of approximately 15,000 kilograms of recycled material. The remaining 11,000 kilograms composed of organic and food waste, are currently not recycled and are assumed to be sent to landfill or incineration, depending on local waste management infrastructure.

Table 17 - Waste diverted from disposal

Waste diverted from disposal 2024	Hazardous waste (kg) - Electronic waste and toner cartridges	Non-hazardous waste (kg)
Preparation for reuse	0	0
Recycling	3,000	12,000
Other recovery operations	0	0

Table 18 - Amount of non-recycled waste (in kg and %)

	Total amount (kg)	Percentage (%)
Non-recycled waste	11,000	42%

Estimation methodology

We estimate the weight of waste generated in our offices using the following approach:

- ↳ **Categorization:** Waste is sorted into key streams (paper/cardboard, plastic, organic, e-waste and residual).
- ↳ **Data collection:** Volumes are recorded based on bin size and collection frequency. When available, we use actual weight data from waste management providers.
- ↳ **Estimation:** In absence of direct weight, we apply standard volume-to-weight conversion factors.
- ↳ **Consolidation:** Data is aggregated regularly across locations to identify trends.
- ↳ **Improvement:** We plan to refine accuracy through digital monitoring, periodic sample weighing.

Bitdefender®

Honoring our people

At Bitdefender, people are at the heart of everything we do, recognizing that the long-term success of the company relies on a motivated and supported team. To cultivate a work environment that encourages innovation and collaboration, we have implemented a series of policies aimed at ensuring a healthy and dynamic organizational climate. Our human resources policies are designed to create an organizational culture where every employee feels valued and can actively contribute to the company's goals and display a behavior in compliance with Bitdefender core values. From well-structured onboarding processes to continuous professional development programs, we ensure that all team members have the resources they need to excel in their respective fields.

In this chapter:

ESRS S1 Own workforce

Strategy

Disclosure Requirement related to ESRS 2 SBM-2 - Interests and views of stakeholders

The company's top management continuously takes measures to implement effective talent management practices in the highly competitive cybersecurity industry, fostering a positive employee experience while ensuring the attraction and retention of top talent. Employee interests and perspectives are integrated into the business strategy, with management providing the necessary support to help individuals and teams achieve and exceed their goals. Managers cascade objectives to their teams, support them in achieving these goals, and adjust them as business needs evolve. Objectives are communicated at the team and individual level to ensure alignment with business priorities.

Disclosure Requirement related to ESRS 2 SBM-3 - Material impacts, risks and opportunities and their interaction with strategy and business model

Material impacts and their link strategy and business model

Employees play an active role in executing the business line's strategy and business model, as approved by top management. Line managers work closely with their teams to assess the impacts, risks, and opportunities related to achieving strategic objectives at the team level. They take measures to mitigate risks of underperformance or non-compliance with company policies and procedures.

Together with support functions, managers ensure full compliance with internal requirements while providing staff with the resources and guidance needed to achieve their objectives and develop a strong career path within the company. Communication between managers and team members is continuous and transparent, covering the business strategy, adopted business model, and the support available to meet targets.

For Bitdefender, the results of the DMA (specifically the identification of material sustainability-related impacts, risks, and opportunities) are directly connected to the company's strategy and business model. These results inform both strategic direction and operational priorities, ensuring that sustainability considerations are embedded in decision-making across the organization.

Positive material impacts on the workforce such as a fair and competitive compensation practices, flexible work arrangements, access to training and skills development programs, and health and well-being initiatives are closely aligned with Bitdefender's strategy and business model. As a technology-driven company, Bitdefender relies on a highly skilled and engaged workforce to deliver innovative cybersecurity solutions. These workforce-focused practices are intentionally integrated into the business model to attract, retain, and empower talent, which is essential to maintaining a competitive edge and driving long-term growth.

As identified through the DMA, certain negative impacts on employees are also directly linked to the company's business model and operating context. Increased workloads for technical, security, and IT operations teams may arise due to the nature of the company's cybersecurity obligations. The constant need to monitor and respond promptly to security incidents can create sustained pressure on these teams, leading to potential stress, fatigue, and long-term well-being concerns.

Furthermore, the company's global operational footprint may negatively affect the work-life balance of employees, especially within technical support functions. Cross-time zone collaboration often requires participation in meetings and communications outside of standard working hours, which may interfere with employees' personal routines and rest periods.

Risks and opportunities arising from impacts and dependencies and their link strategy and business model

The material risks and opportunities arising from impacts and dependencies on Bitdefender's own workforce are closely linked to the company's strategy and long-term competitiveness. As a knowledge-based, innovation-driven organization in the cybersecurity sector, Bitdefender's success is fundamentally dependent on the skills, well-being, and engagement of its workforce. The DMA identified key issues such as talent attraction and retention, employee well-being, digital upskilling, diversity and inclusion, and remote/hybrid work policies as material areas.

These factors shape both risk exposure and strategic opportunity. For instance, the ability to attract and retain top cybersecurity talent in a highly competitive global market is critical to sustaining innovation and customer trust. In response, Bitdefender aligns its human capital development strategy with these findings, investing in employee training, flexible work models, and inclusive workplace practices. This integration ensures that workforce-related sustainability matters are not only managed as risks but also leveraged as strategic assets supporting innovation, operational resilience, and long-term value creation.

The material risks and opportunities arising from impacts and dependencies on people in the company's own workforce do not relate to specific groups of people, but rather to all Bitdefender employees. All people in Bitdefender's own workforce who could be materially impacted by Bitdefender are included in the scope of its disclosure.

Bitdefender's workforce comprises both employees and non-employees who may be subject to material impacts arising from the nature of their engagement or working conditions:

Table 19 - Description of Bitdefender's workforce

Workforce Category	Description
Employees	Full-time (standard weekly schedule) and part-time (reduced hours). Most employees are on permanent contracts, with a small number engaged under fixed-term contracts for specific roles or projects.
Interns	Students or early-career professionals who join the company for a defined period (usually 3 months with the possibility to extend the duration of practice), typically for learning and development purposes. They are usually paid and partially integrated into departmental activities.
Contractors	Owners/administrators of companies with direct contracts with Bitdefender.
Outsourcers	Employees of outsourcing firms contracted to deliver services or processes. Their staff work on company-related tasks but are employed and managed by the external provider.
Project-Based Outsourcers	A subset of outsourcers engaged specifically for time-limited projects. Their activity is closely linked to project timelines and deliverables, often with fluctuating intensity.
Employees of Record (EOR)	Staff working for Bitdefender but employed by an Employer of Record (EOR) provider. This model is typically used to support workforce presence in countries where the company does not have a legal entity. EOR staff are fully integrated operationally but are not under direct employment contracts.

As part of our ongoing commitment to inclusivity, safety, and ethical operations, Bitdefender has undertaken a comprehensive assessment to ensure that our working environment do not pose a risk of harm to individuals with particular characteristics, including but not limited to gender, age, disability, race, or religion. We conduct regular internal reviews and staff surveys to understand the lived experiences of our employees, particularly those from potentially vulnerable groups. All employees undergo mandatory training on diversity, equity, and inclusion, as well as training related to ethical conduct and risk awareness. We consider specific activity contexts, such as remote or hybrid work environments and specific activities stressors (e.g., long screen time, project deadlines) to identify potential occupational health risks. Where applicable, accommodations are made to mitigate these risks. Based on this thorough analysis, we have determined that there are no risks of harm for people with particular characteristics.

Characteristics of material negative impacts

The material negative impacts on Bitdefender's own workforce are not widespread or systemic. They are related to individual incidents rather than recurring or broad-based issues. The company has a robust framework for addressing any such incidents, ensuring that appropriate measures are taken to resolve the situation and prevent similar occurrences in the future. Bitdefender remains committed to maintaining a positive work environment and promoting the well-being of its employees.

Activities that result in positive impacts

The company implements a range of initiatives designed to generate positive impacts across its workforce. These include employee well-being programs, the protection of labor rights, enhanced career development opportunities, and continuous improvement of working conditions. All such actions are intended to benefit all employees and contribute to a supportive, safe, and inclusive working environment.

For additional details, please refer to Disclosure Requirement S1-4 - Taking action on material impacts on own workforce, and approaches to managing material risks and pursuing material opportunities related to own workforce, and effectiveness of those actions.

Impact, risk and opportunity management

Disclosure Requirement S1-1 - Policies related to own workforce

In order to manage its material impacts on its own workforce, Bitdefender has the following policies in place: the Employee Handbook and the Code of Business Conduct.

Code of Business Conduct

The Code of Business Conduct ("The Code") applies to all directors, officers, employees and consultants of Bitdefender Holding B.V. and its subsidiaries. Through the Code, Bitdefender is committed to upholding and promoting the human and labor rights of all individuals within its workforce, in line with the UN Guiding Principles on Business and Human Rights. The company's commitment to respect and promote human rights by upholding these principles in its relationships with its employees, consultants, suppliers and partners is integrated into the Company's Code of Business Conduct.

All employees receive mandatory training on human rights and labor standards upon onboarding and through regular refresher sessions on various topics, such as:

- Sexual Harassment Global Awareness
- Diversity and Inclusion
- Creating an Inclusive Environment
- Code of Business Conduct
- Information Security Awareness
- Data Privacy Awareness

Staff can report concerns without fear of retaliation on Whistleblowing channels and employee representatives have monthly meetings with the Governance and Compliance Advisor where they raise staff concerns and requests to Top Management.

Bitdefender's Code of Business Conduct directs employees toward actions that nurture a culture of integrity, respect, and excellence. By embodying these values each day, employees continuously seek new ways to protect and maintain business operations from both emerging and established threats, thereby enhancing Bitdefender's reputation as a leader in the cybersecurity field.

The management of the Code of Business Conduct Policy, approved by the Human Resources Director, establishes responsibilities throughout the organization to ensure all employees complete specific online training annually on the Code of Business Conduct.

Bitdefender actively fosters open, ongoing communication with its workforce to swiftly identify, address, and resolve human rights issues. The mechanisms for such engagement include open-door policies that encourage employees to report concerns without fear of retaliation, as outlined in Bitdefender's Whistleblowing procedure. Additionally, structured forums and committees in certain regions, such as Bitdefender France, allow employee representatives to bring labor-related or human rights matters to management's attention. This primarily involves the Comité Social et Économique (CSE) Committee, which holds monthly meetings with the HR Governance and Compliance Advisor. During these meetings, they present Bitdefender France's concerns or requests, which are then submitted to top management for resolution and approval. Management is dedicated to thoroughly investigating all reported incidents and applying necessary sanctions as required.

Employee Handbook

The Employee Handbook serves as a comprehensive regulatory and guidance document designed to support employees in fulfilling their roles and responsibilities. It outlines key policies and procedures on the following topics:

- Personal data protection
- Health, hygiene, and occupational safety, including maternity protection
- Compliance with the principle of non-discrimination and the prevention of any form of dignity violation
- Evaluation of professional competencies
- Amicable conflict resolution procedures
- Working hours, rest periods, and related entitlements
- Disciplinary offenses and applicable sanctions
- General training and development policy for employees

The provisions of the Employee Handbook are mandatory for all personnel. The HR Coordinator is responsible for ensuring that each employee reads and understands the handbook upon signing their employment contract. Employees are expected to fully comply with its requirements and can access the latest version via the company intranet.

To ensure effective implementation, Department Heads and Business Vertical Directors assess adherence to the handbook during onboarding evaluations and at the end of the probationary period.

Policy commitments addressing human trafficking, forced or compulsory labor and child labor

Bitdefender's Code of Business Conduct specifically addresses forced labor, trafficking and child labor. The Anti-Slavery and Anti-Human Trafficking provisions of the Code set forth the company's commitment to a work environment that is free from slavery and human trafficking, which includes forced labor and unlawful child labor. Bitdefender will not tolerate or condone slavery or human trafficking in any part of its global organization. Bitdefender employees, contractors, subcontractors, vendors, partners and others through whom Bitdefender conducts business must avoid complicity in any practice that constitutes trafficking in persons or slavery.

Workplace accident prevention policy

Bitdefender has implemented a proactive workplace accident prevention policy to ensure the health and safety of its employees by consistently identifying and mitigating potential risks. Although the nature of the company's activities typically presents a low risk of physical accidents, Bitdefender is steadfast in its commitment to maintaining a safe and compliant work environment. This commitment is realized through preventive measures, comprehensive employee training, and continuous monitoring to uphold the highest safety standards.

Policies aimed at elimination of discrimination and promoting equal opportunities

Bitdefender is an Equal Opportunity Employer that does not discriminate on the basis of actual or perceived race, creed, color, religion, alienage or national origin, ancestry, citizenship status, age, disability or handicap, sex, marital status, veteran status, gender, sexual orientation, genetic information, arrest record, or any other characteristic protected by applicable federal, state or local laws. The Bitdefender management team is dedicated to this policy with respect to recruitment, hiring, placement, promotion, transfer, training, compensation, benefits, employee activities and general treatment during employment.

The principles are included in the **Employee Handbook** (applicable for the U.S., The Netherlands, France and Romania) and made known to employees globally, across the organization, at onboarding and during employment, through the Bitdefender Intranet. The HR Governance and Compliance Advisor and the People Partners disseminate the stipulations of all the HR Policies and commit to supervising compliance with Bitdefender Human Resources policies.

Bitdefender's policy commitments focus on preventing any form of direct or indirect discrimination against employees rather than specifically addressing groups at heightened risk of vulnerability. Nonetheless, the company proactively supports employees facing vulnerable situations, ensuring their needs and concerns are given special consideration. For more details regarding the methods through which Bitdefender continuously engage with employees in vulnerable situations, please refer to Disclosure Requirement S1-2 - Processes for engaging with our workforce and workers' representatives regarding impacts.

Bitdefender is committed to providing reasonable accommodation for qualified employees with disabilities, addressing their known physical or mental limitations. Employees needing assistance to perform their job duties due to physical or mental condition are encouraged to notify their assigned People Partner. Similarly, Bitdefender strives to accommodate employees' sincere religious beliefs, provided this does not create undue hardship for the company's operations.

For any inquiries or concerns about equal employment opportunities, employees are strongly encouraged to reach out to the Global Head of People Partners or report their concerns through the designated whistleblowing channels. Bitdefender is dedicated to ensuring a workplace free from retaliation against those who raise concerns about equal employment opportunities. To foster an environment without artificial barriers, violations of this policy, including retaliatory actions, will result in disciplinary measures, potentially leading to termination of employment. It is crucial that all employees fully cooperate with investigations related to these matters.

Disclosure Requirement S1-2 - Processes for engaging with own workforce and workers’ representatives about impacts

Mode of engagement

Bitdefender continually engages with workers through all the company channels and HR Managers as well as line managers have recurrent meetings and conference calls with employees in which they discuss relevant issues related to employee experience. In these discussions and in employees’ feedback we identified the positive impact of work flexibility offered by the remote and hybrid work policy adopted by the company to retain top talent and enhance their engagement level.

In 2024 we improved the benefits offered to Bitdefender Group, by reviewing and updating the health insurance contracts to include more health services offered to staff, more hours of psychological assistance, sports, which were selected following a staff survey to include their benefits preferences.

Engagement process and responsibilities

The company has processes in place to ensure that employee perspectives inform decision-making. Managers, business line VPs, and People Partners collaborate on talent management programs that support business objectives and help strengthen employee engagement and retention. These programs include regular one-on-one meetings between managers and team members, with People Partners contributing to performance management, career development, succession planning, benefits, and compensation practices.

Managers and the HR team are engaged throughout the employee journey, from recruitment and onboarding to growth and development through coaching and training. They provide opportunities for career development, offer competitive compensation and benefits, conduct performance reviews, and support employees in achieving objectives and building a positive experience at Bitdefender.

Assessing engagement effectiveness

Bitdefender assesses workforce engagement through a combination of formal and informal mechanisms, including employee surveys, feedback on benefits such as health insurance, and other channels for employee input.

In addition, managers maintain ongoing, direct communication with their teams, allowing them to stay attuned to employees’ levels of motivation, personal career aspirations, and the type of support needed to achieve both individual and organizational goals. This two-way dialogue enables the company to respond promptly to concerns, align development opportunities with employee expectations, and foster a culture of open feedback and continuous improvement.

Engaging with vulnerable workforce groups

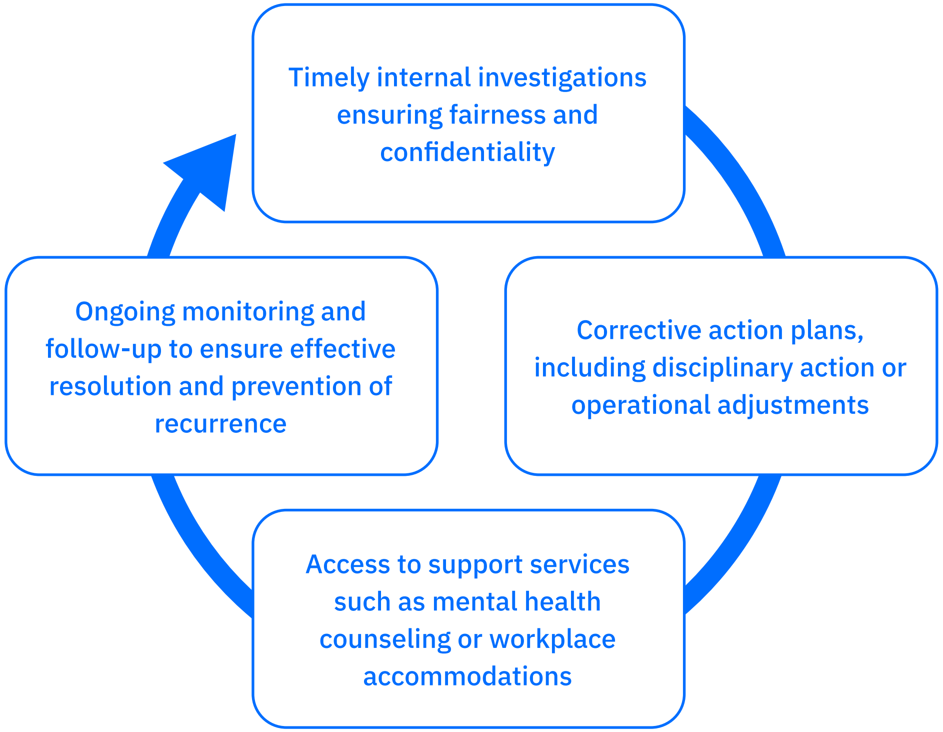
Dedicated People Partners continuously engage with employees in vulnerable situations, paying particular attention to their needs and concerns. For instance, Bitdefender France provided a defibrillator for a disabled employee, allowing her to monitor her heart condition while ensuring the company is prepared for any emergency interventions. Additionally, for migrant employees requiring working visas, our Legal Department facilitates visa acquisition, with People Partners overseeing the process to ensure timely completion for the commencement of work at Bitdefender.

Disclosure Requirement S1-3 - Processes to remediate negative impacts and channels for own workforce to raise concerns

Approach and process for remediation

As part of our commitment to responsible business conduct and respect for human rights, Bitdefender has established clear processes to provide for or cooperate in the remediation of negative impacts on people within our workforce. These measures align with the UN Guiding Principles on Business and Human Rights and reflect our ongoing efforts to promote a safe and inclusive workplace.

Where Bitdefender identifies that it has caused or contributed to a material negative impact including but not limited to discrimination, harassment, health and safety concerns or unfair labor practices, we initiate a formal remediation process that includes:



Timely internal investigations ensuring fairness and confidentiality

Corrective action plans, including disciplinary action or operational adjustments

Access to support services such as mental health counseling or workplace accommodations

Ongoing monitoring and follow-up to ensure effective resolution and prevention of recurrence

Channels for raising concerns and grievance mechanisms, including availability

Bitdefender provides multiple, accessible grievance and feedback mechanisms for our employees to raise concerns and seek resolution. We provide a secure whistleblower channel available 24/7 that allows employees to report their concerns. Bitdefender's employees are encouraged to approach their direct managers or HR representatives to report their concerns openly. Our internal digital platform provides a structured form for submitting ethics-related concerns, workplace incidents, or policy violations. Employees can choose to identify themselves or remain anonymous.

Bitdefender has a formal grievance and complaints handling mechanism in place specifically for employee related matters. This mechanism is designed to ensure that all employees have a safe, confidential, and accessible way to raise concerns, report misconduct, or seek resolution for workplace issues.

Bitdefender ensures that grievance and complaints handling mechanisms are not only available, but also accessible, trusted, and effective for all employees. To support the consistent availability and use of these channels, the company has implemented the following key processes: Grievance procedures are embedded in Employee's handbook and The Code of Business Conduct. All employees are informed of available channels during onboarding and through regular internal communications.

Tracking and monitoring effectiveness

Bitdefender tracks the effectiveness of its initiatives through a variety of feedback channels and workforce data. Employees can provide input on workplace experience, including well-being and stress, through the performance review process. We also consider retention trends, participation in wellness and training programs, and employee feedback on leadership.

Assessment of awareness and trust in the mechanisms for raising concerns

The company assesses awareness and trust in its internal grievance and reporting mechanisms through employee training, surveys, and regular communication campaigns. These efforts aim to ensure that all members of the workforce understand how to raise concerns and feel confident that their issues will be addressed fairly and without negative consequences.

The Code of Business Conduct includes a strict non-retaliation policy, which applies to all individuals, including employees, contractors, and workers' representatives, who report concerns in good faith. To reinforce this commitment, the company monitors all reported cases for any indications of retaliatory behavior.

Oversight of this policy is ensured by the Ethics team, which operates independently and reports directly to the board, further strengthening accountability and trust in the process. These measures are designed to foster a culture of transparency and psychological safety, encouraging employees to speak up without fear.

CO$_2$

Disclosure Requirement S1-4 - Taking action on material impacts on own workforce, and approaches to managing material risks and pursuing material opportunities related to own workforce, and effectiveness of those actions

Bitdefender adopts a proactive approach in managing the significant impacts, risks, and opportunities associated with our workforce. Our comprehensive action plans are designed with a strong emphasis on enhancing employee well-being, ensuring workplace safety, and promoting professional growth. By prioritizing these areas, we aim to create an environment where employees feel supported and valued, contributing positively to both their personal development and the company's success. Through regular assessments and updates to our strategies, we remain agile in addressing any challenges and seizing potential opportunities, ensuring Bitdefender's workforce thrives in a dynamic and secure atmosphere.

Actions taken to mitigate negative impacts

As part of the Double Materiality Assessment, Bitdefender has identified negative impacts related to the work-life balance of its employees. The demanding nature of cybersecurity requirements, coupled with the urgency of responding swiftly to incidents, can lead to overtime and after-hours work for technical, security, and IT operations teams. Furthermore, the need for continuous availability to support global collaboration may lead to meetings and communications outside regular business hours, disrupting the daily routines of technical support teams.

Regarding workload, managers reviewed roles, positions and job descriptions in their teams to ensure they have human resources with the right skills and expertise in each role in their team and constantly evaluated their workload. Staff also work in shifts in roles where they need to provide continuous technical support to Bitdefender customers, team managers' reports on the 24-hours technical support are submitted monthly for the payment of the overtime, according to local labor legislation and compensation plans signed by staff.

Actions aimed at delivering positive impacts

Bitdefender has established multiple initiatives to deliver positive impacts for its workforce. These include employee development programs, such as regular skills training, leadership development, and access to business certifications.

Table 20 - Actions aimed at delivering positive impacts and resources allocated

Action	Description	Resource allocated to impact management
Health monitoring	Bitdefender is doing its best to provide stability and high-quality life for employees by providing insurance, health care, parental leaves and work accidents.	Bitdefender invests substantial resources in managing its material impacts on the workforce. This includes a dedicated budget for employee welfare programs such as wellness initiatives and skills development, as well as structural resources like flexible work arrangements, remote work options, on-site wellness facilities, and employee assistance programs.
Ergonomic improvements	We do regular assessments and improvements to workstations, including ergonomic chairs, adjustable desks, and proper lighting. The Bitdefender ergonomics program is heavily focused on preventative measures to reduce the risk of work-related musculoskeletal disorders. This includes ergonomics training sessions for our team members and providing input into the purchase or design of work equipment, systems, and facilities to ensure that they meet ergonomic standards to provide the best levels of efficiency, comfort, health and safety for anyone using them.	
Wellbeing programs	Office massage for employees that includes a 15-minute session of back massage, done by a climatotherapist on a special massage chair. This aims to reduce stress and back pain, increase blood circulation and boost energy.	

Tracking the effectiveness

To ensure ongoing effectiveness, Bitdefender maintains continuous monitoring through regular follow-up with affected employees, employee surveys focused on stress levels, and an annual review of work policies. Bitdefender tracks and assesses the effectiveness of these initiatives through multiple methods. Key performance indicators such as employee satisfaction scores, retention rates, and program participation rates are regularly monitored. Bitdefender also evaluates the usage of wellness and training programs and monitors leadership performance through employee feedback.

Actions to mitigating material risks

As part of our Double Materiality Assessment, Bitdefender has not identified any material risks for the company arising from its impacts and dependencies on its own workforce to date. However, we maintain active risk management, product oversight, and user feedback mechanisms to detect and address potential future impacts, should they arise. These include regular privacy impact assessments, product safety reviews, and engagement with customer support and incident reporting systems.

Actions to pursue material opportunities

Through our Double Materiality Assessment, Bitdefender has identified an opportunity in enhancing employee trust and loyalty by implementing advanced technologies and stringent security measures to protect employee data. Bitdefender continues to ensure that all personal employee data remains confidential, with access to Human Resources Management (HRM) systems strictly limited to the individual employee and the HR Data Analyst. Additionally, our Information Security (InfoSec) Team enforces comprehensive policies that rigorously control access to personal staff data, reinforcing our commitment to safeguarding employee privacy and fostering a trustworthy work environment.

Metrics and targets

Disclosure Requirement S1-5 - Targets related to managing material negative impacts, advancing positive impacts, and managing material risks and opportunities

Bitdefender has established workforce-related targets designed to reduce material negative impacts, strengthen positive contributions, and address key risks and opportunities. Current priorities include minimizing job loss and mitigating its effects on departing employees, and promoting health and safety in the workplace. These targets were approved in 2024 for an initial one-year period, with progress monitored by line managers on a weekly, monthly, and quarterly basis.

It is important to note that the current scope and design of these targets are not yet fully aligned with the requirements of the ESRS. Bitdefender is committed to reevaluating and refining them in future reporting cycles to ensure greater consistency with ESRS standards and to further enhance the company's management of workforce-related impacts, risks, and opportunities.

Table 21 - Targets related to Bitdefender's own workforce

Area	Target	Relevance	Progress
Support for Departing Employees	Provide 100% of laid-off employees with outplacement services, severance, and wellbeing support.	Maintains company reputation and eases transitions.	HR and Line managers offered full support to 100% of departing employees by severance agreements, payment of legal fees, extension of health insurance and transparent, supportive communication after the exit.

Area	Target	Relevance	Progress
Health and Safety	Zero workplace accidents and occupational illnesses, both for our employees and for our collaborators.	Reflects Bitdefender's commitment to safeguarding the health, safety, and well-being of both employees and collaborators, while ensuring compliance with legal requirements and aligning with international best practices on workplace safety	In 2024, we achieved our target of zero workplace accidents and occupational illnesses for our employees and for our contractors, outsourcers or partners operating on our sites.

Process for setting health and safety targets

At Bitdefender, the process for setting health and safety targets begins by conducting a comprehensive assessment of health and safety risks, including ergonomic evaluations, mental health assessments, and cybersecurity related health risks such as exposure to excessive screen time or musculoskeletal disorders. Bitdefender engages its own workforce in this process, including:

- Software development team, support, management and remote workers;
- Workers' representatives and a dedicated health and safety committees with representatives from HR, management and workers' representatives.

We use a variety of methods to ensure workforce engagement such as ergonomics workshops, meetings where employees can share health and safety concerns or suggest improvements or feedback channels. Also, the Health and Safety Bitdefender's committee has monthly meetings, which include representatives from management and the workforce. Based on the feedback collected, the Health and Safety committee sets specific, measurable, relevant and time-bound targets such as reducing or eliminating work-related injuries and occupational diseases, reducing the number of near misses, ensuring 100% of employees complete health and safety training or achieving 100% compliance in employees' health checks. Bitdefender commits to continuously reviewing and updating its health and safety targets based on workforce feedback, and regulatory requirements.

Disclosure Requirement S1-6 - Characteristics of the undertaking's employees

Key characteristics of Bitdefender's own workforce

Bitdefender's own workforce consists primarily of employees hired under direct employment contracts, including both full-time and part-time staff. Most employees are on permanent contracts, with a small number engaged on a fixed-term basis. The workforce includes a mix of roles across technical, operational, and support functions, with a presence in multiple countries. Key workforce characteristics, including headcount, gender distribution, contract types, regional breakdown, and employee turnover, are detailed in the following sections.

Table 22 - Total number of employees by head count, and breakdowns by gender

Gender	Number of employees (head count)
Male	1,445
Female	618
Total Employees	**2,063**

Table 23 - Total number of employees by head count, and breakdown by country

Country	Female	Male	Total
Australia	1	1	2
Denmark	-	1	1
Dubai	-	4	4
France	15	39	54
Germany	7	20	27
Indonesia	10	34	44
Italy	1	7	8
Malaysia	1	-	1
Netherlands	4	5	9
Other	-	2	2
Romania	507	1,167	1,674
Singapore	18	25	43
Spain	7	9	16
UK	4	15	19
US	43	116	159

Country	Female	Male	Total
Grand Total	**618**	**1,445**	**2,063**

Table 24 - Employees by contract type, broken down by gender

Contract type	Female	Male	Total
Number of employees	618	1,445	2,063
Number of permanent employees	590	1,366	1,956
Number of temporary employees	28	79	107
Number of non-guaranteed hours employees	0	0	0
Number of full-time employees	601	1,414	2,015
Number of part-time employees	17	31	48

In 2024, a total of 269 individuals left the company. This includes all contract types and all forms of departure (e.g., resignation, end of contract), resulting in a turnover rate of 13%. The turnover figure includes interns, who are typically employed on fixed-term contracts of three months, with the possibility of extension or conversion to permanent roles. Due to the inherently temporary nature of these contracts, interns contribute disproportionately to the number of leavers and can artificially increase the turnover rate.

To provide a clearer view of core workforce stability, an adjusted turnover rate was calculated excluding interns. This results in a turnover rate of approximately 11%, reflecting only the departures of employees under direct and ongoing employment contracts. This dual-perspective approach (with and without interns) enhances transparency and provides a more accurate picture of workforce dynamics, particularly in the context of sustainability reporting. Both calculations are based on verified internal HR data and follow commonly accepted HR analytics standards.

Methodologies and assumptions

The workforce-related data presented in this Statement are compiled based on internal HR systems and reflect the company's own employees only (i.e., individuals hired under direct employment contracts). The following methodological choices were applied:

Headcount vs. Full-Time Equivalent (FTE): The employee data is reported based on headcount, meaning everyone is counted as one employee, regardless of working hours (i.e., both full-time and part-time employees are counted equally as one headcount unit).

In certain internal analyses, we may also report on a Full-Time Equivalent (FTE) basis, where:

- ↳ 1.0 FTE = one full-time employee (based on a standard 40-hour workweek)
- ↳ Part-time employees are converted proportionally based on their contractual working hours (e.g., an employee working 20 hours/week = 0.5 FTE)
- ↳ Unless otherwise specified, disclosures in this report refer to headcount.

Reporting Reference Point: The data reflects the actual headcount at the end of the reporting period (as of December 31, 2024). This approach was chosen to provide a clear and verifiable snapshot of the workforce and is consistent with our internal HR reporting practices. For certain indicators such as employee turnover, an average headcount across the year is used as the basis for calculation, in order to reflect changes over time more accurately.

Contextual information

The total number of employees has shown steady growth between 2022 and 2024, increasing from 1,677 employees in 2022 (1,196 male and 481 female) to 1,735 employees in 2023 (1,226 male and 509 female), and reaching 2,063 employees in 2024 (1,445 male and 618 female).

This growth is primarily attributed to the company's strategic expansion in technical and commercial areas. The increase in technical staff (from 912 employees in 2022 to 1,035 in 2024) and commercial staff (from 404 employees in 2022 to 554 in 2024) reflects the demand for enhanced innovation, product development, and market presence. Growth in administrative and other support roles has also supported business scalability. Top management numbers remained relatively stable, with a slight increase aligned to organizational restructuring to support expanded operations.

During the reporting period, the workforce evolved both in size and composition. Fluctuations across the reporting periods are mainly driven by business expansion initiatives, strengthening of sales and marketing functions, and ongoing investments in technical expertise.

While overall headcount followed a steady upward trend, turnover levels remained relatively stable compared to the previous year. These combined dynamics reflect a growing organization with ongoing recruitment efforts, natural attrition, and cyclical intern contracts contributing to workforce movement throughout the year.

The company performs monthly headcount reconciliations between the HR and Finance teams to ensure alignment in workforce reporting. These reconciliations are based on internal HR records and financial reporting requirements. However, different methodologies are applied depending on the reporting purpose:

For financial reporting purposes, the headcount includes employees, contractors, and Employer of Record (EOR) staff, reflecting the full operational workforce supporting the business. For sustainability reporting purposes, only employees under direct employment contracts and paid interns are included, in line with ESG reporting standards. Although the scope differs, the data used in both cases is based on validated internal HR records, ensuring consistency, transparency, and accuracy within each respective reporting framework.

Disclosure Requirement ESRS S1-7 - Characteristics of non-employees in the undertaking's own workforce

Key characteristics of non-employees Bitdefender's own workforce

In addition to its directly employed workforce, Bitdefender's operational model also leverages contributions from various non-employee categories, including contractors, outsourcers, project-based outsources, and Employees of Record (EOR).

These individuals support specific business needs but are not engaged under direct employment contracts, and are not included in the company's payroll systems, and the internal HR team does not maintain full, detailed records regarding their contractual terms, compensation, or working conditions.

Consequently, these non-employee categories are most often excluded from formal workforce reporting metrics (such as headcount, turnover, and demographic analyses), which focus exclusively on directly hired employees.

While contractors are excluded from official external reporting, they may be included separately in certain internal analyses when relevant for operational purposes. However, they remain distinct from the employee population.

As of December 31, 2024, Bitdefender's workforce included 110 non-employees, compared to 103 non-employees in 2023. This change represents a 6.8% year-over-year increase. The variation is attributed to normal business activity fluctuations. No exceptional events or structural workforce changes materially impacted on the number of non-employees during the reporting period. This covers:

- ↳ Self-employed individuals (contractors) who have direct commercial agreements with Bitdefender to provide highly specialized services.
- ↳ Individuals employed by outsourcing or staffing companies contracted by Bitdefender for operational support or specific projects.
- ↳ Employees of Record (EORs), who are fully integrated into Bitdefender's operational structure but legally employed by third-party Employer of Record providers.

Interns are reported separately and considered part of Bitdefender's own workforce due to the potential for transitioning to direct, fixed-term employment after completing their internship period.

The non-employee data is reported based on headcount, meaning everyone is counted as one employee, regardless of working hours (i.e., both full-time and part-time employees are counted equally as one headcount unit).

In certain internal analyses, we may also report on a Full-Time Equivalent (FTE) basis, where:

- ↳ FTE = one full-time employee (based on a standard 40-hour workweek)
- ↳ Part-time employees are converted proportionally based on their contractual working hours (e.g., an employee working 20 hours/week = 0.5 FTE)
- ↳ Unless otherwise specified, disclosures in this Sustainability Statement refer to headcount.

Reporting Reference Point: The data reflects the actual headcount at the end of the reporting period (e.g., as of December 31, 2024). This approach was chosen to provide a clear and verifiable snapshot of the workforce and is consistent with our internal HR reporting practices. For certain indicators such as employee turnover, an average headcount across the year is used as the basis for calculation, to reflect changes over time more accurately.

Disclosure Requirement ESRS S1-9 - Diversity metrics

Bitdefender is committed to fostering an inclusive, equitable, and diverse workplace that reflects the broader society in which we operate. To provide a transparent view of our workforce composition, we present below the gender distribution at top management level, along with the overall employee age distribution across the company.

Gender distribution at top management level

Bitdefender values gender diversity at all organizational levels, including top leadership. As of December 31, 2024, the gender distribution at the top management level is as follows:

Table 26 - Gender distribution in top management

Category	Number	Percentage
Women in top management	7	21.2%
Men in top management	26	78.8%
Total top management headcount	**33**	**100%**

This reflects the company’s ongoing efforts to promote gender balance and support the advancement of women in leadership positions.

Age distribution of the workforce

As of December 31, 2024, Bitdefender employed a total of 2,063 individuals under direct employment contracts. This age profile of the workforce is presented in the table below and demonstrates a dynamic and predominantly mid-career workforce, with a strong representation of young professionals.

Table 27 - Age distribution of Bitdefender’s employees

Category	Number	Percentage
Under 30 years old	670	32.5%
30 to 50 years old	1,293	62.7%
Over 50 years old	100	4.8%

Disclosure Requirement ESRS S1-10 - Adequate wages

All Bitdefender employees are paid at or above the legal minimum wage in every country where we operate. Through internal benchmarking, we aim to ensure that the vast majority of employees receive wages that are adequate and aligned with relevant local standards and cost-of-living benchmarks. We conduct an annual compensation review process and are currently undertaking a detailed wage adequacy assessment, in line with applicable standards. Should any discrepancies be identified, we will transparently disclose the countries and percentages concerned in the next reporting cycle.

In 2024 we also focused on internal and external benchmarking of staff salaries and allocated a dedicated Rewards team to the salaries benchmarking analysis and measures that were taken to have a consistent rewards policy throughout the company. Managers submitted requests for salary increases based on staff performance and salary benchmarking data in the industry.

Regarding non-employees (such as contractors, outsourcers, and employees of record), Bitdefender requires its third-party partners to comply with applicable labor laws, including ensuring the payment of adequate wages. While we do not directly manage their compensation, we are committed to promoting fair labor practices across our extended workforce.

Disclosure Requirement ESRS S1-12- Persons with disabilities

Due to varying legal and data privacy restrictions, Bitdefender does not collect or process disability-related data for employees in all jurisdictions. Consequently, it is not possible to determine the percentage of persons with disabilities among employees subject to these legal limitations. This constraint is particularly significant in countries with strict privacy laws or limitations on processing sensitive personal data without explicit consent, including but not limited to:

- France, Germany, Italy, Spain, Netherlands, Denmark (in line with EU GDPR requirements)
- United Kingdom (post-Brexit UK GDPR)
- United States (where ADA and state laws may restrict employer data collection)
- Australia, Singapore, Indonesia, Malaysia, and Dubai (where privacy legislation imposes similar restrictions)
- As of December 31, 2024, Bitdefender employed a total of 5 individuals with disabilities, representing approximately 0.24% of the company’s total workforce of 2,063 employees. As a result of the previously mentioned facts, the disclosed figures for employees with disabilities (0.24% of the workforce, based on self-disclosure and legally allowed records) reflect only jurisdictions where collection is permitted and individuals have consented.

Bitdefender remains committed to respecting the privacy of all employees while advancing diversity, equity, and inclusion in every country of operation.

Table 28 - Number of persons with disabilities employed

Gender	Count of Gender	Percentage
Female	1	0.05%
Male	4	0.19%
Grand Total	**5**	**0.24%**

Disclosure Requirement S1-13 - Training and skills development metrics

Bitdefender has a company-wide performance and career development process in place, which is designed to apply to all employees across all levels and functions. The process is supported by formal tools and regular cycles, and the majority of employees are covered by this framework, benefiting from structured discussions around their performance and professional growth.

In a highly competitive industry, attracting and retaining top talent is a key priority for Bitdefender. Our talent management approach also emphasizes continuous learning and development, offering hard and soft skills training tailored to business needs and supported by line managers.

For compliance with the Code of Business Conduct and the company values, for ensuring diversity and inclusion, staff complete mandatory trainings such as:

- Code of Business conduct
- Code of Social Media Conduct (HR policy)
- Information Security (InfoSec Policy and Training)
- Workplace Respect (International)
- Diversity and Inclusion
- Creating an Inclusive Environment
- Sexual Harassment: Global Awareness

While the company does not currently track participation rates with a level of granularity that would allow detailed reporting by gender or employee category, efforts are being made to strengthen data availability for future reporting cycles.

In total, over **7,200 training hours** were delivered to **818 unique employees**, resulting in an average of slightly under **9 hours of training per participant** throughout the year.

Table 29 - Average number of training hours by gender

Gender	Average number of training hours
Female	Just above 8 hours
Male	Just above 9 hours

Table 30 - Average number of training hours per employee category and by gender

Category	Female Employees	Male Employees
Administrative	Just above 8 hours	Almost 9 hours
Commercial (Sales & Marketing)	About 8 hours	Almost 8 hours
Others (Support roles)	Around 3 hours	Just above 4 hours
Technical	Around 10.5 hours	Around 11 hours
Top Management (C&VP level)	Less than 1 hour	Nearly 12 hours

These figures reflect Bitdefender's ongoing investment in employee learning and development, tailored to each function's needs and responsibilities.

It is worth noting that, beyond the mapped training sessions, several employees are enrolled in longer-term development initiatives whose duration and structure do not allow for easy inclusion in the training hours data, but which contribute meaningfully to professional development.

Disclosure Requirement S1-14 - Health and safety metrics

Bitdefender's entire workforce is covered by a Health and Safety management system that complies with legal requirements and aligns with recognized international guidelines. In 2024, **no work-related accidents**, **occupational illnesses**, **or fatalities were recorded among our employees working on-site**. The company also recorded **zero fatalities among non-employees**, such as contractors, outsourcers, or partners operating on Bitdefender premises.

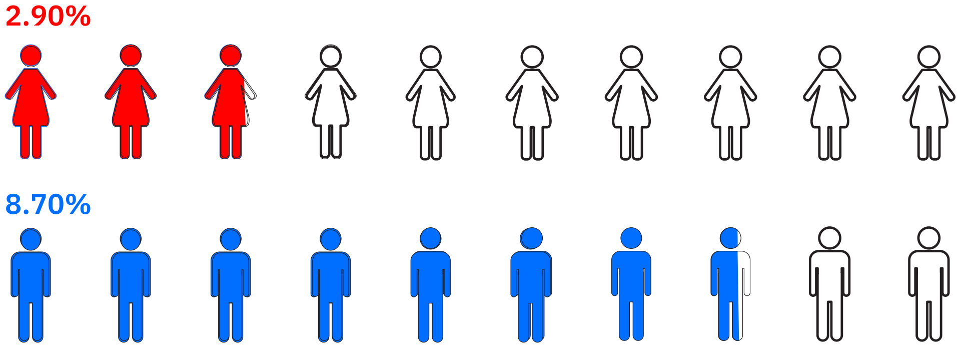
At the end of 2024, no employee illnesses were attributed to Bitdefender's activities. This result reflects our strong commitment to maintaining a safe and healthy work environment. Furthermore, no days of sick leave were reported as a result of workplace accidents or occupational diseases during the year.

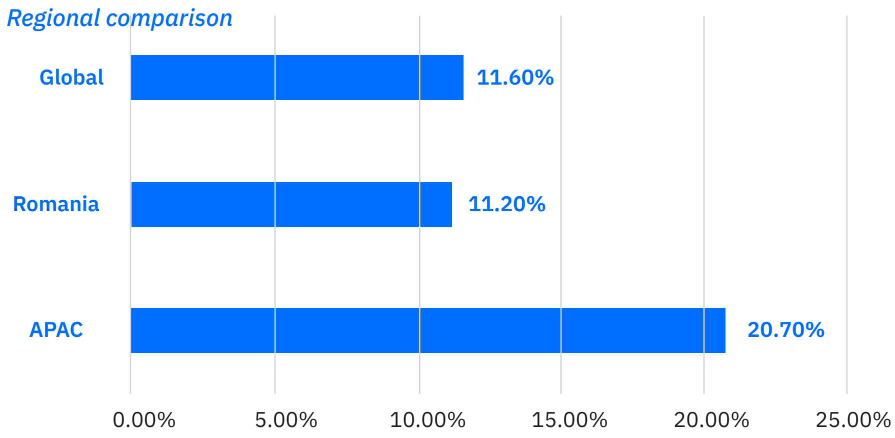
ESRS S1-15 - Work-life balance metrics

Bitdefender offers family-related leave entitlements in full compliance with national labor legislation and internal human resources policies. These leave types are designed to support employees in balancing their personal and professional responsibilities and typically include maternity, paternity, and adoption leave, as well as time off to care for a dependent or attend to significant family events (marriage, death of a family member etc).

All of the company's employees (100%) are entitled to family-related leave under national labor legislation and internal HR policies. This type of leave includes maternity, paternity, and adoption leave, as well as time off to care for a dependent or to attend family-related events (e.g. marriage, bereavement, or child illness).

Employees who made use of family-related leave in 2024
(Total 11.6%)





The percentage of employees who took family-related leave was calculated based on the number of unique employees who made use of at least one such leave during the reporting period. Multiple absences taken by the same employee were counted only once in order to reflect the proportion of the workforce affected, not the total number of leave requests.

Disclosure Requirement S1-16 - Remuneration metrics (pay gap and total remuneration)

Gender pay gap

Bitdefender is committed to fair and transparent pay for all employees, and we regularly monitor how pay is distributed across the organization. As part of this process, we assess two key indicators: the gender pay gap, which compares average pay between women and men, and the pay ratio, which compares the highest-paid individual to the typical employee. These measures provide insights into our current position and highlight areas for improvement in building a more equitable and inclusive workplace.

At the company level, the overall gender pay gap in 2024 was 21%, meaning that, on average, female employees earned 21% less than male employees across the organization. This outcome reflects differences in gender representation across job levels and functions and does not indicate unequal pay for equal work.

It is important to emphasize that the gender pay gap presented here reflects overall pay differences and should not be interpreted as a direct measure of pay equity for employees performing equivalent roles. Comparisons of equal pay for equal work are addressed separately through internal assessments.

Contextual information

The gender pay gap was calculated using gross annual full-time equivalent (FTE) remuneration, with part-time salaries normalized to ensure consistent comparison across the workforce. All employees under direct employment contracts as of December 31, 2024, were included, while contractors, outsourcers, and Employees of Record were excluded. Remuneration covers gross annual pay, including fixed and variable components under formal compensation plans, such as structured sales incentives. Discretionary bonuses, awarded on a case-by-case basis, were excluded due to a lack of centralized tracking but may be incorporated in future reporting once global data collection improves.

Disclosure Requirement S1-17 - Incidents, complaints and severe human rights impacts

During the reporting period, two incidents of alleged discrimination were recorded, one in the United States and one in Romania. The U.S. case, raised by a former employee, was formally withdrawn. In Romania, the investigation concluded that there was no evidence of discriminatory treatment or harassment; however, it highlighted the need to provide greater clarity around workplace relationships and responsibilities.

Bitdefender takes all allegations of discrimination seriously and is firmly committed to upholding human rights and work-related rights across all operations. Every case is addressed through fair and transparent processes, with the aim of ensuring a safe, respectful, and inclusive workplace for all employees.

ESRS S4 Consumers and end-users

Strategy

Disclosure Requirement related to ESRS 2 SBM-2 - Interests and views of stakeholders

Bitdefender integrates the interests, rights, and perspectives of its consumers and end-users into its strategy and business model through a multifaceted approach that emphasizes data protection, ethical conduct, and user engagement.

1. Commitment to Consumer Privacy and Data Protection

Bitdefender places a strong emphasis on safeguarding user privacy, aligning its practices with international data protection standards such as the EU General Data Protection Regulation (GDPR). The company's privacy policies detail the types of personal data collected, the purposes for which data is used, and the rights of users regarding their information. Bitdefender ensures that personal data is processed lawfully, transparently, and for specific purposes, reflecting its commitment to respecting the rights of its users.

2. Ethical Business Practices and Human Rights Considerations

The company's Code of Business Conduct underscores its dedication to integrity, honesty, and compliance with applicable laws and regulations. This code serves as a framework guiding employees to uphold ethical standards, avoid conflicts of interest, and engage in fair business practices. By fostering a culture of responsibility, Bitdefender ensures that its operations respect the rights and interests of all stakeholders, including consumers and end-users.

3. User Engagement and Feedback Mechanisms

Bitdefender actively engages with its user base to understand their needs and concerns. The company provides multiple channels for users to seek support, offer feedback, or raise issues, including online support centers and community forums. This ongoing dialogue allows Bitdefender to adapt its products and services to better serve its users, ensuring that their voices inform strategic decisions.

4. Transparency and Accountability in terms and conditions results in the use of solutions and services

Through clear and comprehensive subscription agreements and terms and conditions, Bitdefender communicates the scope of its services, user responsibilities, and the measures in place to protect user data and rights. These documents outline the company's obligations and the mechanisms available to users for dispute resolution, reflecting Bitdefender's commitment to transparency and accountability.

Disclosure Requirement related to ESRS 2 SBM-3 - Material impacts, risks and opportunities and their interaction with strategy and business model

Bitdefender acknowledges that actual and potential impacts on consumers and end-users, particularly in areas such as data privacy, digital security, online safety, and responsible use of technology, are inherently interconnected with the company's strategy and business model. As a global cybersecurity provider, the nature of our products and services directly influences the digital safety and experience of individual users, families, and businesses. Therefore, managing these impacts is not peripheral but central to how Bitdefender creates value and maintains trust.

There is a continuous process through which insights from impact assessments and stakeholder feedback inform and contribute to the adaptation of our strategy and business model. This includes integrating considerations such as secure-by-design product development, and responsible innovation into both short- and long-term strategic planning. Our product roadmap, customer support practices, and external engagement activities are routinely adjusted based on emerging risks, evolving user expectations, and societal trends, ensuring a proactive and accountable approach to sustainability-related impacts.

Bitdefender's strategy and business model are directly influenced by the material risks and opportunities arising from its impacts and dependencies on consumers and end-users. As a cybersecurity company, our success depends on maintaining user trust, ensuring product reliability, and upholding data protection and privacy standards (areas that also represent key sustainability-related dependencies).

The risks and opportunities are embedded in strategic planning, product development, and user engagement processes, ensuring that Bitdefender's offerings remain responsive, responsible, and aligned with both societal needs and business resilience. As part of our ESG evolution, these considerations are increasingly reflected in investment decisions, partnerships, and market positioning strategies.

Consumers and/or end-users subject to material impacts

Bitdefender's assessment and disclosure processes aim to include all consumers and end-users who are likely to be materially impacted by the company's operations, products, services, and business relationships. This scope encompasses:

- ↳ Direct end-users of Bitdefender's cybersecurity solutions (individuals, families, and businesses),
- ↳ Users indirectly affected through third-party distribution channels, OEM partnerships, and integration with other platforms,
- ↳ Individuals impacted through data collection, threat intelligence, and automated decision-making systems,
- ↳ And consumers affected by value chain practices, including outsourced service providers and technology partners.

Bitdefender operates in a global digital environment, where any individual or organization with an internet-connected device can be considered a potential consumer or end-user of its cybersecurity solutions. This includes users from all geographies, sectors, and demographic groups, ranging from individual consumers and families to small businesses and large enterprises.

Given the nature of Bitdefender's products and services, there is a particular focus on safeguarding users' data rights, digital autonomy, and online safety. Special attention is also directed toward vulnerable groups, including children using internet-connected devices, recognizing their increased exposure to online risks.

Material negative impacts on consumers or end-users

As of 2024, Bitdefender has not identified any material negative impacts on consumers or end-users stemming from its operations, products, or activities within its value chain. The company remains dedicated to continuous monitoring and active stakeholder engagement to ensure any potential impacts are addressed proactively.

Material positive impacts on consumers or end-users

Bitdefender's solutions aim to generate positive outcomes, particularly by enhancing digital safety, mitigating cyber threats, and empowering users to navigate the online environment securely. As part of its 2024 Double Materiality Assessment, the company has identified several material positive impacts:

Table 31 - Material positive impacts on consumers or end-users

Material positive impacts	Description of the activities that result in positive impacts, types of consumers and/or end-users positively affected and geographic scope
To safeguard user privacy, Bitdefender has implemented an End User Anonymization Policy and established a dedicated department to ensure full GDPR compliance	Bitdefender's End User Anonymization Policy and dedicated GDPR compliance department ensure lawful and transparent data processing. These measures are embedded in product design, data handling, and governance, demonstrating a commitment to default and design data protection. **Activities Leading to Positive Impacts**: ↳ **Data minimization and anonymization** to reduce privacy risks while maintaining functionality for threat detection and product enhancement. ↳ **Privacy-by-design architecture** integrating safeguards at all stages, from endpoint detection to cloud threat intelligence. ↳ **Dedicated GDPR oversight** with continuous audits, impact assessments, staff training, and engagement with regulators. **Types of Consumers and End-Users Positively Affected**: These initiatives benefit a wide spectrum of users globally, including: ↳ Individual consumers concerned with digital privacy and surveillance, ↳ Children and families, whose data is particularly sensitive and protected, ↳ Enterprises and SMEs, which rely on Bitdefender to meet regulatory obligations and protect client data, ↳ Vulnerable or at-risk groups, including persons with limited digital literacy or in regions with weaker privacy enforcement. **Geographic Scope:** Although designed to meet EU GDPR standards, the company applies these privacy principles globally, ensuring equal protection for users worldwide (including North America, Latin America, and Asia-Pacific). This approach reduces data misuse risks and fosters trust, transparency, and ethical data stewardship.

Material positive impacts	Description of the activities that result in positive impacts, types of consumers and/or end-users positively affected and geographic scope
Ensuring user security through cybersecurity products (versus third-parties), including scam prevention	Bitdefender’s mission is to protect users from cyber threats with advanced cybersecurity solutions, including malware detection, phishing prevention, identity protection, and real-time threat response, integrated into its consumer and business products. **Activities Leading to Positive Impacts**: ↳ **Real-Time Threat Detection:** AI-driven intelligence and global telemetry block malware and phishing scams before reaching users. ↳ **Anti-Scam Features:** Anti-phishing, fraud alerts, and URL filtering protect against identity theft and financial loss. ↳ **Secure-by-Design:** Tools focus on user protection and system performance, ensuring security and accessibility. ↳ **User Education**: Blogs, newsletters, and guidance help users identify and avoid scams. **Types of Consumers and End-Users Positively Affected**: Individual consumers facing scams, phishing, and ransomware. ↳ Non-tech-savvy users susceptible to social engineering. ↳ Families protected through parental controls. ↳ SMEs without dedicated IT security facing digital threats. ↳ Users in regions with low digital resilience impacted by fraud and malware. **Geographic Scope:** Bitdefender products are available in over 170 countries, with major user bases in Europe, North America, Latin America, and Asia-Pacific.

Material positive impacts	Description of the activities that result in positive impacts, types of consumers and/or end-users positively affected and geographic scope
Bitdefender ensures the protection of B2B customer information through strict access controls and the exclusive use of tools that comply with the company's privacy policy and are approved by the information security team.	Bitdefender enforces strict access control protocols in B2B operations to protect customer information, supporting its commitment to responsible data governance and cybersecurity. **Activities Leading to Positive Impacts**: ↳ **Restricted Access**: Only authorized personnel can access B2B customer data, with role-specific needs, robust authentication, and monitoring controls. ↳ **Tool Approval**: Bitdefender mandates tools comply with privacy and security standards for handling customer data. ↳ **Policy Enforcement**: Regular audits, access reviews, and employee training ensure adherence to global regulations like GDPR. **Types of Consumers and End-Users Positively Affected**: These measures are particularly beneficial to Bitdefender's B2B clients, which include: ↳ SMEs and large enterprises operating in sectors with sensitive data (e.g. healthcare, finance, legal), ↳ Channel partners and managed service providers, who rely on Bitdefender's tools to secure their own customers, ↳ Organizations in regulated industries that face high compliance requirements and require verifiable data protection measures from vendors. **Geographic Scope:** Bitdefender applies these access controls and approval processes globally, with a consistent policy framework across Europe, North America, Asia-Pacific, and other key regions. This global application enhances customer confidence and supports secure data operations across borders.

Material positive impacts	Description of the activities that result in positive impacts, types of consumers and/or end-users positively affected and geographic scope
Bitdefender fosters strong customer relationships by offering dedicated B2B and B2C support services, engaging openly through social media channels, and leveraging monitoring tools (e.g., Social Sprout) to respond proactively to customer needs	**Bitdefender's Communication Approach**: Bitdefender emphasizes direct and transparent communication with B2B and B2C customers through support services, digital channels, and social media monitoring to foster trust and improve user experience. **Activities Leading to Positive Impacts**: ↳ **Multilingual Support**: Real-time support via email, chat, and phone assists users with technical, product, and account inquiries. ↳ **Social Media Interaction**: Open engagement on platforms like X, Facebook, LinkedIn, and Instagram provides assistance, educational content, and security alerts, building digital trust. ↳ **Dedicated Customer Relations**: Specialized teams ensure personalized support for corporate and consumer engagements globally. ↳ **Social Monitoring Tools**: Tools like Sprout Social help identify trends, gather feedback, and address emerging issues, enhancing communication strategies. **Types of Consumers and End-Users Positively Affected**: This multi-channel support system benefits: Individual consumers and families seeking fast and accessible cybersecurity guidance, ↳ Non-technical users who may require more hands-on assistance or language-specific support, ↳ Business customers, who depend on reliable vendor communication for operational continuity, ↳ Potential and existing customers engaging with Bitdefender through public or informal channels. ↳ **Geographic Scope**: Customer support services and social engagement practices are global, with support offered in multiple languages across key regions including Europe, North America, Latin America, and Asia-Pacific.

Material positive impacts	Description of the activities that result in positive impacts, types of consumers and/or end-users positively affected and geographic scope
By providing VPN solutions, Bitdefender helps customers access information safely and reliably, protecting their privacy and data security	Bitdefender’s Virtual Private Network (VPN) solutions play a critical role in promoting secure, private, and unrestricted access to digital content and information. These services are designed to protect user identity, enhance data privacy, and circumvent regional restrictions or censorship, thus contributing to digital rights and information freedom. **Activities Leading to Positive Impacts**: ↳ **Privacy and Anonymity**: Bitdefender VPN encrypts user traffic and masks IP addresses, protecting users from tracking, surveillance, and data interception, particularly important when using public or unsecured networks. ↳ **Secure Remote Access**: VPN solutions also benefit remote workers, digital nomads, and global enterprises, allowing secure access to company networks and online platforms regardless of physical location. **Types of Consumers and End-Users Positively Affected:** Bitdefender’s VPN solution benefits: ↳ Everyday internet users concerned about privacy and digital freedom, ↳ Residents of countries with restricted or censored internet access, ↳ Journalists, activists, and human rights defenders seeking secure and uncensored communication, ↳ Businesses with remote teams, requiring secure and reliable access to internal systems across borders. **Geographic Scope:** Privacy-focused VPN services are global.

Material positive impacts	Description of the activities that result in positive impacts, types of consumers and/or end-users positively affected and geographic scope
Bitdefender’s customers receive continuous access to information and updates about their subscriptions, along with non-commercial communications on security breaches and protection activities	Bitdefender ensures clear and responsible communication with users, offering real-time updates, threat alerts, and educational information to enhance protection in a digital world. **Activities Leading to Positive Impacts**: ↳ **Subscription Updates**: Users receive timely notifications about subscriptions and service availability via the interface, email, and Bitdefender Central. ↳ **Breach and Threat Alerts**: Proactive, non-commercial alerts inform customers of threats, breaches, and cyber risks, enhancing awareness and security. ↳ **Privacy-Respecting Messages**: Communications are relevant, non-intrusive, and aligned with user privacy preferences, providing accessible information. ↳ **Security Transparency**: Users are informed of protection actions like threat blocks and system scans, fostering trust through transparency **Types of Consumers and End-Users Positively Affected**: These communication practices benefit: ↳ Individual consumers and families, who are supported with relevant and timely security updates, ↳ Non-technical users, who may not proactively seek security information but benefit from simplified notifications, ↳ B2B customers, who rely on clear and timely alerts to manage their own IT security processes, **Geographic Scope:** This positive impact are global in reach. Language localization and multi-platform support ensure that users in diverse contexts benefit equally from these communications.

Material positive impacts	Description of the activities that result in positive impacts, types of consumers and/or end-users positively affected and geographic scope
Bitdefender enhances customer security and satisfaction by providing timely reports and information, effectively managing detection and response through its cybersecurity solutions, and delivering dedicated customer success management for the B2B segment	Bitdefender delivers tailored B2B services that empower organizations to understand, manage, and improve their cybersecurity posture. These include detailed customer reports, advanced threat detection and response (MDR/EDR/XDR) solutions, and dedicated customer success management. **Activities Leading to Positive Impacts**: ↳ **Reporting and Dashboards:** Provides business clients with real-time updates on threat activity, device status, incident response, and security compliance. ↳ **Managed Detection and Response (MDR):** Offers 24/7 threat monitoring, analysis, and response to quickly detect and neutralize cyber threats. ↳ **Customer Success Management**: Assigns specialized CSMs to guide B2B clients in deployment, solution optimization, and maximizing cybersecurity investments. ↳ **Proactive Advisory Support**: CSMs and security analysts offer tailored industry-specific recommendations to enhance cybersecurity maturity. **Types of Consumers and End-Users Positively Affected**: These services primarily support: ↳ Small and medium-sized businesses (SMBs) and large enterprises with limited internal cybersecurity capacity, ↳ Organizations in critical sectors such as healthcare, finance, education, and government, where cybersecurity failures have broad impacts, ↳ Global partners and managed service providers (MSPs), who rely on Bitdefender's tools and guidance to protect their downstream clients. **Geographic Scope:** Bitdefender's B2B support and managed services are offered globally. Localized customer success resources and regional threat intelligence ensure that clients receive contextually relevant support, regardless of geography.

Material positive impacts	Description of the activities that result in positive impacts, types of consumers and/or end-users positively affected and geographic scope
Bitdefender provides parental control solutions that protect minors from harmful online content and offer reporting mechanisms to support safe digital use	Bitdefender offers dedicated parental control solutions aimed at safeguarding minors from harmful or inappropriate content online. These tools empower parents and guardians to protect children's digital well-being, encourage responsible internet use, and prevent exposure to online risks, including cyberbullying, exploitation, and age-inappropriate content. **Activities Leading to Positive Impacts**: ↳ **Content Filtering and Access Restrictions**: Bitdefender's parental controls allow families to filter and block harmful or inappropriate content, manage screen time, and set age-appropriate restrictions across devices. ↳ **Real-Time Activity Monitoring**: Parents can monitor online activity in real time, enabling timely intervention if a child engages with risky content or platforms. ↳ **Reporting Mechanisms**: Bitdefender provides tools for parents to report inappropriate behavior or potential threats, contributing to faster remediation and improved product response. ↳ **User Education and Alerts**: The platform educates parents about emerging digital threats and provides tips for fostering safe online habits in children. **Types of Consumers and End-Users Positively Affected:** ↳ Families with children and adolescents who require supervised digital engagement, ↳ Non-technical parents or guardians seeking user-friendly security solutions to protect minors, ↳ Children and young users who benefit directly from reduced exposure to harmful digital environments. **Geographic Scope:** Bitdefender's parental protection tools are available to global B2C users, with language and content filtering capabilities adapted for use across Europe, the Americas, Asia-Pacific, and other regions. The solution is especially impactful in areas where cyber risks to minors are heightened or where digital literacy is still developing.

Material positive impacts	Description of the activities that result in positive impacts, types of consumers and/or end-users positively affected and geographic scope
Bitdefender implements technological support programs for start-ups, students and NGOs, while facilitating access to cybersecurity business solutions at a discounted price	Bitdefender supports digital inclusion and cybersecurity empowerment by offering discounted access to its business-grade cybersecurity solutions for start-ups, students, and non-governmental organizations (NGOs). These programs help bridge the cybersecurity gap for under-resourced or early-stage entities, ensuring that more organizations and individuals can protect their data and operations in a rapidly evolving digital landscape. **Activities Leading to Positive Impacts**: ↳ **Discounted Programs**: Offers start-ups, students, and NGOs reduced-cost access to cybersecurity tools to safeguard operations within limited budgets. ↳ **Technical Guidance**: Provides onboarding support, best-practice advice, and product documentation to ensure effective tool utilization. ↳ **Supporting Innovation**: Secures early-stage companies and educational communities to promote safer innovation and reduce digital economy vulnerabilities. ↳ **Community Impact**: Helps NGOs protect sensitive data, defend against cyber threats, and maintain trust in healthcare, education, and humanitarian sectors. **Types of Consumers and End-Users Positively Affected**: ↳ Students and academic communities, especially those studying or building careers in IT and cybersecurity, ↳ NGOs and non-profits, particularly those working with vulnerable populations or handling personal/sensitive data. **Geographic Scope:** These programs have a global reach.

Material risks and opportunities for Bitdefender arising from impacts and dependencies on consumers and/or end-users

In today’s rapidly evolving digital landscape, the company is exposed to a wide range of material risks and opportunities arising from its interactions and dependencies with consumers and end-users worldwide. These considerations apply across all user groups globally, rather than being limited to specific demographics or age segments. The table below outlines Bitdefzender’s material risks and opportunities, detailing their origins from impacts and dependencies on consumers and end-users, as well as the strategies implemented to mitigate or pursue them.

Table 32 - Material risks and opportunities arising from impacts and dependencies on consumers and/or end-users

Material risks/opportunities	Description
Risk: Privacy breaches, mishandling or unauthorized access to customer data can determine reputational, financial and market risks	Bitdefender operates in a domain where trust and data protection are fundamental to its relationship with consumers and end-users. The company is highly dependent on its ability to handle customer data securely and transparently across its cybersecurity product ecosystem. As such, any privacy breach or mishandling of personal data—whether due to internal system failure, human error, or external attack—can directly lead to material reputational, financial, and regulatory consequences. This risk originates from both the impact Bitdefender could have on users (through potential misuse or exposure of data) and the company's dependency on user trust and data accuracy to deliver effective security services. Given that many of Bitdefender's solutions process sensitive or personal information (e.g. threat detection logs, device activity, location data), a loss of integrity or confidentiality can significantly harm consumer confidence and undermine product performance.
Risk: AI implementation determines the change of business processes and operations (market risk)	The integration of Artificial Intelligence (AI) into Bitdefender's cybersecurity products and operations introduces both strategic opportunities and market risks. This risk emerges from dependencies on consumer expectations, trust, and user behavior, as well as the potential impacts of AI-driven decisions on end-users. As Bitdefender increasingly relies on AI to enhance threat detection, automate responses, and personalize user experiences, there is a dependency on end-user data quality and behavior patterns to train and refine these systems. At the same time, users depend on Bitdefender to ensure that AI-driven outputs are accurate, unbiased, transparent, and do not compromise user autonomy or privacy. Any failure to meet these expectations—such as an AI system incorrectly flagging threats, misclassifying safe content, or creating a lack of transparency—can lead to: Loss of consumer trust, ↳ Regulatory scrutiny (particularly under AI and data governance frameworks), ↳ Market resistance to adoption, or ↳ Reputational harm linked to unintended impacts on end-users. ↳ These are material risks that stem from both Bitdefender's impact on users via automated systems and its reliance on end-user interaction and trust for AI adoption.

Material risks/opportunities	Description
Opportunity: Evaluations by independent institutions can enhance customer trust and differentiation (reputation, market share)	Bitdefender's opportunity to enhance customer trust and differentiate in the cybersecurity market through independent evaluations arises directly from its dependencies on consumer trust and expectations, as well as the positive impact such transparency has on end-user confidence. Consumers and end-users of cybersecurity solutions depend on reliable, independently validated information to make informed choices about the protection of their digital lives and assets. Bitdefender's success, therefore, depends on its ability to demonstrate credibility, effectiveness, and compliance in a crowded and highly technical market.

For actions to mitigate material risks and pursue material opportunities, please see Disclosure Requirement S4-4 - Taking action on material impacts on consumers and end- users, and approaches to managing material risks and pursuing material opportunities related to consumers and end-users, and effectiveness of those actions.

Impact, risk and opportunity management

Disclosure Requirement S4-1 - Policies related to consumers and end-users

To effectively manage the material impacts of its products and services, as well as the associated material risks and opportunities, Bitdefender has developed and continually updates a comprehensive ecosystem of policies, procedures, and internal guidelines. The part of this ecosystem relevant to consumers and end-users includes a **Code of Business Conduct** and a **Privacy Policy**.

Code of Business Conduct outlines the company's commitment to data protection, describing how it safeguards personal information globally. The policy adheres to principles ensuring lawful, transparent, and secure data handling, with commitments to minimize data collection, ensure accuracy, limit retention, and maintain confidentiality. Procedures emphasize lawful and fair data practices, retaining information only for legitimate purposes, and implementing rigorous security measures against unauthorized access. For more information regarding the Code of Business Conduct, please refer to Disclosure Requirement G1-1- Business conduct policies and corporate culture.

This Bitdefender Privacy policy applies globally and explains the personal data we process, how and where we may use it, how we protect it, who has access to it, with whom we share it, and how to exercise your privacy rights. This privacy policy also complies with the applicable data protection legislation, such as the EU General Data Protection Regulation (GDPR - Regulation 2016/679), as well as other data protection requirements in any of the jurisdictions where Bitdefender operates.

Respect for the Human Rights of Consumers and End-Users

Bitdefender is committed to respecting and promoting internationally recognized human rights across all areas of its operations, including its relationships with consumers, end-users, partners, and suppliers. This commitment is formally grounded in the UN Guiding Principles on Business and Human Rights, which the company explicitly upholds, and is reflected in processes that align with both the OECD Guidelines and the ILO Declaration, even where not directly cited.

1. General Commitments

Bitdefender affirms its respect for human dignity, autonomy, privacy, and safety of all individuals engaging with its services and products. Through its Code of Conduct, Bitdefender upholds the principle that business success must be earned through honesty, integrity, and lawful behavior, with an ethical obligation to prevent harm to stakeholders — including consumers.

2. Privacy and Data Protection

Bitdefender explicitly safeguards confidential personal information of stakeholders, including consumers and retirees, maintaining it under strict confidence and in compliance with applicable law.

The Code of Conduct emphasizes adherence to all laws, rules, and regulations in jurisdictions where it operates — this includes data protection regulations such as GDPR, which are integral to respecting consumer rights in the digital space.

Bitdefender's Privacy Policy outlines its adherence to data protection legislation, including the EU General Data Protection Regulation (GDPR). Key practices include:

Data Minimization and Purpose Limitation
Collecting only necessary personal data for specified purposes

Anonymization and Pseudonymization
Implementing measures to anonymize or pseudonymize data to protect user identities

No Data Selling Policy
Committing not to sell user data to third parties

User Rights
Ensuring users can access, rectify, or delete their personal data, and providing mechanisms to exercise these rights

3. Engagement with Consumers and End-Users

Trust, Credibility & Accessibility	Speak-Up Culture	Due Diligence in Supply Chain and Product Design
Bitdefender's Code of Conduct promotes a culture of openness, trust, and transparent engagement, encouraging all stakeholders — implicitly including end-users — to raise ethical concerns.	Although designed primarily for employees, Bitdefender's "Speak-Up" culture and open communication values foster a climate in which stakeholder feedback is valued, including from consumers where relevant (e.g., user safety issues, ethical concerns, or service-related impact).	Through its Anti-Slavery and Anti-Trafficking policy and Conflict Minerals clause, Bitdefender ensures that its products are not associated with labor or human rights abuses — protecting end-user integrity and aligning with the OECD's human rights due diligence expectations. Suppliers are contractually required to uphold these same standards, ensuring that products offered to consumers are ethically sourced, lawfully produced, and free of exploitation.

Disclosure Requirement S4-2 – Processes for engaging with consumers and end-users about impacts

General process for engagement

Bitdefender engages with consumers and end-users through a comprehensive, multi-channel approach aimed at identifying, assessing, and addressing both actual and potential impacts on their rights and interests. This includes proactive communication, transparent product information, accessible feedback mechanisms, and targeted initiatives to ensure that consumer concerns are heard, understood, and acted upon in a timely and responsible manner.

1. Consumer Solutions Group

On the Consumer Solutions Group, Bitdefender provides multiple avenues for consumers to communicate concerns, seek assistance, and provide feedback

- ↳ Our exhaustive **knowledge** base Bitdefender Support Center translated in 11 languages: English, French, German, Italian, Spanish, Romanian, Portuguese (Brazilian and European), Dutch, Swedish, traditional Chinese
- ↳ **24/7 Live Chat Support**: Accessible via the Bitdefender Support Center, offering real-time assistance for various issues in any language both human and AI.
  - ↳ **Email Support**: Users can submit inquiries or report issues through email in English, French, German, Italian, Spanish, Romanian, Portuguese (Brazilian and European), and Dutch, Swedish, traditional Chinese
  - ↳ **Phone Support**: Users can call regional support numbers provided on the support page.
  - ↳ **Community Forums**: The Bitdefender Expert Community allows users to discuss topics, share experiences, and receive guidance from both peers and Bitdefender representatives.

- ↳ **Social Media Platforms**: Bitdefender maintains active profiles on platforms such as Facebook, Twitter, and Instagram, where users can engage with the company and stay informed about updates.
- ↳ **Through our B2C indirect partners or our B2B2C partners Customers Services** - the general processes for how Bitdefender Consumer Support engages with B2C and B2B2C users are described in https://www.bitdefender.com/consumer/support/technical-b2b2c/

Feedback and Surveys

To continuously improve its products and services, Bitdefender solicits feedback from users:

- ↳ **Post-Support Surveys**: After resolving support tickets, Bitdefender sends detailed surveys to users to assess satisfaction and identify areas for improvement.
- ↳ **Public Review Platforms**: Users are encouraged to share their experiences on platforms like Trustpilot and Gartner Peer Insights providing transparency and insights into customer satisfaction.

Continuous Improvement and Accountability

Through its engagement mechanisms, Bitdefender seeks to identify and address potential impacts on consumers and end-users:

- ↳ Responsive Support: The company’s support infrastructure allows for timely resolution of issues, minimizing potential adverse effects on users.
- ↳ Product Updates and Enhancements: Feedback from users directly influences product updates, ensuring that Bitdefender’s offerings remain effective and aligned with user needs.

2. Business Solutions Group

On the Business Solutions Group, Bitdefender provides 24x7 Technical Support services for Bitdefender Business Products, in English language, world-wide, with our HQ based engineers.

Bitdefender also offers localized support in our France, Germany, Romania, Spain and US points of presence. For these, Support is offered in local language, within business hours.

Full Support contact details can be found at Contact Enterprise Support.

Main Enterprise Support Channels are:

- ↳ Phone, chat and email support available 24/7 in English.
- ↳ Community Forum - through our Bitdefender Expert Community
- ↳ Web form - Business customers can submit a Support Case via the Bitdefender web form. You will be able to submit a Case to Bitdefender Support by using the contact form from the support area of the website, following this link.
- ↳ CustomerZone - Bitdefender’s main customer support portal for Business customers.

Other channels:

- ↳ Social Media Platforms: Reddit, Facebook, Twitter, Linkedin and Instagram.
- ↳ Feedback & Surveys:
- ↳ Post Call customers - At the end of a call with a support engineer the customer is asked to provide his feedback about the latest support interaction.
- ↳ Email Surveys - Emails automatically generated after a support case has been resolved.

All this information is also available in our Enterprise Support Policy.

Engagement with stakeholders with affected consumers and/or end-users or their representatives

The company integrates end-user feedback into risk, harm, and benefit assessments through direct channels (Early Access Programs, advisory boards, post-incident reviews) and indirect channels (support trend analysis, surveys, telemetry data). Engagement effectiveness is tracked via metrics such as NPS, participation rates, and usage analytics.

During the current reporting period, end-user perspectives gathered through our GravityZone Early Access Programs (EAPs) have directly influenced product development and strategic decisions across multiple initiatives. For a recent project, for example, feedback from 50+ selected organizations guided enhancements in ML-based hardening logic and attack surface reduction workflows to better align with real-world IT environments.

Both formal and informal interactions with customers, including those serving vulnerable groups in sectors like healthcare and education, ensure solutions are adaptable to diverse needs. The Customer Experience and Product teams oversee these activities, with Product teams accountable for outcomes.

Disclosure Requirement S4-3 - Processes to remediate negative impacts and channels for consumers and end-users to raise concerns

Our overarching approach to addressing any material negative impact on consumers or end-users is centered around delivering timely and effective remediation through robust support mechanisms. When we identify that our services have caused or contributed to such an impact, we place customer satisfaction at the core of our response process.

To ensure the remedy is effective, we actively engage with affected customers throughout the support journey. We also collect and analyze feedback through post-support surveys to determine whether their concerns have been fully resolved, and their overall experience has improved. This continuous feedback loop allows us to refine and improve our response processes over time.

Effectiveness is further measured through key performance indicators such as response time, customer satisfaction scores, and Net Promoter Score (NPS).

Our direct support channels are continuously monitored, with incident response protocols in place to guarantee 24/7 availability. In the event of a system outage affecting one or more support channels, alternative contact options are made available to ensure uninterrupted assistance. For more details on the channels in place for consumers to communicate their concerns or needs directly with the company, seek assistance, and provide feedback, please see Disclosure Requirement S4-2 - Processes for engaging with consumers and end-users about impacts.

All customer cases are managed via a centralized Customer Relationship Management (CRM) platform. This system ensures full traceability of interactions, enables real-time tracking of response times and issue resolution, and facilitates internal communication on user-impacting issues. The CRM also supports timely updates to customers, helping to set clear expectations regarding resolution timeframes.

Most of the feedback coming from business customers is consolidated within a support case. Each case is first evaluated to assign a severity based on the impact reported that determines its priority. The definition for each severity is included in our Enterprise Support Policy .

Scenario example

In case of a usability issue, we first try to reproduce the scenario internally and report it to the Engineering team to be analyzed and if applicable, resolved with a product update.

In case of a cybersecurity flaw, the feedback is reported to the Bitdefender Labs to be analyzed and quickly remediate it.

In case of data privacy concerns, the case will be evaluated together with our privacy team and a best course of action is taken within a timely manner.

In case of product enhancements, these cases are reported to the Product Management team to be analyzed and if accepted the new feature will be included in a future release.

For all cases which are marked as an incident, the Incident Management flow is initiated at the BSG level. All product related incidents are announced to customers through our GravityZone status page.

To demonstrate our commitment to safeguarding customer data, we maintain compliance with internationally recognized information security standards. The company holds **SOC 2 Type 2** certification, which validates the effectiveness of our internal controls related to security, availability, and confidentiality over time. Additionally, we are certified under **ISO 27001**, the global standard for information security management systems, and **ISO 27017**, which provides specific guidelines for cloud service security. These certifications reflect our ongoing efforts to uphold best practices in data protection, mitigate cybersecurity risks, and build trust with our customers through transparent and robust security governance. All certifications are available here.

Disclosure Requirement S4-4 - Taking action on material impacts on consumers and end- users, and approaches to managing material risks and pursuing material opportunities related to consumers and end-users, and effectiveness of those actions

Understanding the significance of material impacts on consumers and end-users is crucial for fostering trust and maintaining business integrity. Bitdefender is committed to recognizing and managing these impacts through proactive measures.

Identifying and Responding to Negative Impacts

Identifying appropriate action in response to a particular actual or potential negative impact on consumers and end-users is a key component. Once users have contacted us using one of the contact channels, their requests are funneled in our CRM for tracking and response purposes.

The CRM also has the ability to classify cases based on source, issue type, severity and what Bitdefender technologies are involved in the creation of negative impact on end users. Once the case has been properly labeled and categorized, it will be handled by an appropriate team with specific training, knowledge, resources. Cases reach different support tiers, based on the labels and categories described above and severity of the reported case.

For Enterprise Support we have the following process:

Enterprise customers provide feedback through multiple channels, including support cases, social media, and surveys. The Enterprise Support team monitors these daily, offering 24/7 assistance and classifying each case to determine appropriate actions.

- ↳ **Product bugs** - Support collects all necessary data, collaborates with Engineering, and deploys fixes either in scheduled releases or, for critical issues, through emergency updates.
- ↳ **Security vulnerabilities** - Support works with customers and Bitdefender Labs to release updates as quickly as possible, with deployment frequency depending on threat detection and malware database updates.
- ↳ **Other concerns** - Issues such as misleading marketing practices are handled in collaboration with Legal and PR teams.

Escalation protocols route cases to the appropriate internal teams when needed, and customers can request escalation via dedicated channels or through Account Managers/Sales Representatives.

For the Consumer Solutions Group, remediation processes are documented and accessible to Customer Support staff according to specialization and tier. Staff use internal tools to investigate and resolve common issues, with both documentation and tools regularly updated based on new products, portfolio changes, industry standards, and feedback from customers and partners. Effectiveness of these actions is measured through key metrics such as response time, customer satisfaction, and Net Promoter Score (NPS).

Actions to Avoid Causing or Contributing to Material Negative Impacts

The company has not identified any material negative impacts on consumers or end-users to date. Nonetheless, it maintains proactive risk management, product oversight, and user feedback mechanisms to identify and address potential future impacts. These include regular privacy impact assessments, product safety reviews, and engagement through customer support and incident reporting systems.

When issues are reported, the company commits to timely resolution, often involving multiple internal teams such as Engineering, Product Management, Labs, Legal, PR, and Privacy. Cases are pursued until a satisfactory resolution is confirmed by the user during support interactions and through post-support surveys.

The company actively works to avoid causing or contributing to negative impacts in areas such as marketing, sales, and data usage, guided by principles of ethical business conduct, consumer protection, and data privacy.

Key practices include:

Responsible marketing and sales

Adhering to strict internal guidelines to ensure product claims are accurate, verifiable, and free from fear-based tactics, while promoting transparency around capabilities and limitations.

Privacy and responsible data use

Embedding data protection from the outset of product development, collecting and processing personal data in compliance with GDPR, CCPA, and other applicable laws, minimizing data collection, and applying strong security controls.

Opt-out and consent management

Providing clear, accessible tools for managing communication preferences, data sharing, and tracking, with continuous updates across platforms.

Third-party due diligence

Requiring vendors and partners to meet strict privacy and ethical standards, with contractual data protection clauses and regular audits.

Incident prevention and reporting

Maintaining protocols to detect, report, and respond to complaints or ethical concerns. To date, no severe human rights or consumer impact incidents have occurred.

Training and accountability

Delivering onboarding and regular training on privacy, ethical marketing, and human rights, with compliance monitored through audits, reviews, and performance evaluations.

Through these measures, the company preserves consumer trust not only by delivering reliable products but also by ensuring fair, transparent, and respectful treatment at every stage of the customer relationship.

Resources allocated to the management of material impacts

Bitdefender allocates dedicated human, financial, and technical resources to manage the material impacts associated with its operations on affected communities, particularly in the areas of digital inclusion, data privacy, cybersecurity awareness, and online safety. The Sustainability function, supported by cross-functional teams from Legal, Product, HR and marketing, is responsible for implementing programs that address these impacts. These resources are reviewed annually and adjusted based on evolving risks, stakeholder feedback, and regulatory developments, ensuring that Bitdefender’s impact management approach remains effective and responsive.

Actions to mitigate material risks and pursue material opportunities

Table 33 - Actions to mitigate material risks and pursue material opportunities

Material Risk description	Planned or underway actions to mitigate material risks for Bitdefender arising from its impacts and dependencies on consumers and/or end-users and how it tracks effectiveness in practice
Privacy breaches, mishandling or unauthorized access to customer data can determine reputational, financial and market risks	To mitigate material risks related to mishandling or unauthorized access to customer and end-user data—which could result in reputational, financial, and market-related consequences- Bitdefender has implemented a Business Continuity Policy and a comprehensive compliance and data protection framework. This framework includes alignment with the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other applicable local regulations, all of which are integrated into our internal set of policies. Key mitigation actions include: ↳ Mandatory onboarding training for all staff on data protection, privacy regulations, and responsible handling of customer data. ↳ GDPR-compliant agreements with all vendors, ensuring that data processors meet strict security and confidentiality standards. ↳ The Legal department drafts privacy policies and terms, offers continuous legal guidance to the Data Protection Officer (DPO), and ensures that all customer-related contracts are reviewed and signed following standardized legal procedures. ↳ The DPO leads the implementation of data protection policies across the business, supported by ongoing oversight and operational integration. ↳ Third-party audits of critical partners are conducted annually, alongside SOC 2 and ISO/IEC 27001 certifications, to validate the effectiveness of information security controls and ensure external compliance. ↳ The Information Security team supervises communications with prospects prior to contract execution to prevent data misuse or unauthorized disclosure. ↳ Opt-out mechanisms are in place for all written communications, with continual improvements made to these features across Bitdefender's websites and internal systems, enabling transparent consent management and respecting user preferences. ↳ The company monitors the effectiveness of these mitigation measures through a combination of audit findings, staff training completion rates, contractual compliance reviews, and feedback from privacy assessments and certification processes.

Material Risk description	Planned or underway actions to mitigate material risks for Bitdefender arising from its impacts and dependencies on consumers and/or end-users and how it tracks effectiveness in practice
AI implementation determines the change of business processes and operations (market risk)	To mitigate the material market risk associated with the implementation of Artificial Intelligence (AI)—specifically the potential disruption or unintended consequences on business processes and operations—Bitdefender has established a multi-layered control and oversight framework. Key mitigation actions include: ↳ The company enforces global policies that govern critical operational domains to ensure organizational consistency, accountability, and compliance across all functions affected by AI-driven change. ↳ The Business Applications department provides ongoing training sessions to relevant internal stakeholders on key operational areas such as user access management, change management, and system governance. This is a continuous process designed to support smooth transitions and enhance system adoption. ↳ All machine learning (ML) algorithms are subject to regular re-evaluation, with performance tracked using defined KPIs and exception reports. Each deviation from expected norms triggers an investigation to identify and correct underlying issues or inaccuracies. ↳ The company maintains detailed documentation in Confluence covering all data flows, processing logic, and data transformations that inform AI-driven reports. This documentation is regularly updated and accessible to relevant teams to ensure traceability and transparency. ↳ Guidelines issued by various internal stakeholders govern the use and integration of AI tools, ensuring alignment with operational needs and ethical standards. ↳ Select AI tools are subject to formal review and approval by both the Legal and Information Security departments to ensure compliance with privacy regulations, cybersecurity protocols, and contractual obligations. ↳ Bitdefender tracks the effectiveness of these mitigation actions through continuous monitoring of model performance metrics, audit logs, feedback from end-users, training participation data, and compliance reviews. This proactive oversight helps ensure that AI implementations deliver value while minimizing operational and market risks.

Material Opportunity description	Planned or underway actions to pursue material opportunities for the company in relation to consumers and/or end-users
Evaluations by independent institutions can enhance customer trust and differentiation (reputation, market share)	Bitdefender recognizes that strong performance in independent third-party evaluations is a key driver of consumer trust, competitive differentiation, and market expansion. As a consistent leader in these evaluations, we are actively pursuing opportunities to enhance visibility, strengthen brand reputation, and expand our customer base by leveraging these strengths. Key actions underway include: ↳ Marketing and communications campaigns that showcase Bitdefender’s top rankings in independent security tests (e.g., AV-TEST, AV-Comparatives), with tailored messaging for different consumer segments and geographies. ↳ Integration of third-party test results and awards into product packaging, websites, sales materials, and enterprise pitches to reinforce customer confidence and influence purchasing decisions. ↳ Strategic collaboration with independent testing institutions to better understand evolving criteria and ensure our products remain aligned with the most rigorous performance standards. ↳ Use of test performance data to inform product roadmap decisions, emphasizing the continuous improvement of capabilities that drive differentiation (e.g., malware detection, low system impact, threat response time). ↳ Proactive public relations efforts and media engagement to amplify recognition from independent bodies and position Bitdefender as a trusted advisor in cybersecurity and digital trust. ↳ Partnership enablement, where our leadership in testing is used to build stronger relationships with channel partners, resellers, and OEMs, offering them a competitive advantage when bundling or reselling our solutions. ↳ Pursuing industry awards and certifications beyond testing (e.g., trust marks, innovation awards) to further validate our leadership and increase brand equity. ↳ These actions not only help Bitdefender grow its consumer and business customer base, but also reinforce our market share and pricing power by positioning our solutions as high-quality, trustworthy, and independently validated

Metrics and Targets

Disclosure Requirement S4-5 - Targets related to managing material negative impacts, advancing positive impacts, and managing material risks and opportunities

Bitdefender has not yet established formal, time-bound and outcome-oriented targets specifically related to its impacts on consumers and/or end-users.

We recognize the importance of setting measurable objectives to enhance our accountability and transparency in managing these impacts, particularly in the areas of digital inclusion, cybersecurity education, and responsible technology access. Bitdefender is committed to establishing formal targets in these areas, with clear timelines and outcome indicators, by the end of 2026, as part of our evolving sustainability strategy.

At present, Bitdefender has not established formal processes specifically designed to track the effectiveness of its policies and actions in relation to material sustainability-related impacts on affected communities. However, the company does monitor a range of Key Process Indicators (KPIs) and Key Risk Indicators (KRIs) through its internal operational workflows and quality assurance systems.

These indicators primarily focus on operational performance, including service delivery, internal compliance, and product integrity, rather than directly measuring progress on sustainability-related impacts or community-level outcomes. They are part of our broader internal controls framework and support risk management and continuous improvement across key business functions.

Governance and compliance

Bitdefender firmly believes that strong governance is essential for driving business success. Throughout the years, we have refined our governance framework to not only meet regulatory standards but also align with our strategic objectives effec-tively. Our dedication to ethical business practices is grounded in strict compliance with legal and regulatory mandates in every market we serve. We ensure that every team member is well-versed in both group-wide and company-specific poli-cies, as well as the regulations pertinent to their roles. Policies are meticulously crafted with input from relevant departments and, upon approval by senior man-agement, disseminated internally and externally when necessary. This compre-hensive approach supports the highest integrity standards across our operations, laying a robust foundation for sustained success and ethical advancement.

In this chapter:

ESRS G1 Business conduct

Governance

Disclosure Requirement related to ESRS 2 GOV-1 - The role of the administrative, management and supervisory bodies

The CEO, as the highest executive authority, is responsible for setting the strategic direction of the company and ensuring that ethical business conduct is embedded across all operations. This includes the development and implementation of ESG policies, which reflect the organization's commitment to sustainability, integrity, and social responsibility. The CEO is responsible for overseeing ESG-related risks, including legal, financial, and reputational, which may impact the company's business conduct and long-term performance. The Risk & ESG Project Manager manages the risk lifecycle at Bitdefender, covering processes from identification and assessment to monitoring and reporting. Additionally, team leaders and CxOs also share ownership of these risks.

Furthermore, the CEO ensures that business conduct principles are integrated into the overall corporate strategy and oversees the preparation and communication of ESG reports, promoting transparency and ethical governance.

The Supervisory Board of Bitdefender Holding B.V. acts as the highest governance body with oversight responsibility for management's conduct and the organization's broader impact on the economy, environment, and society. It ensures that appropriate standards of business ethics and compliance are upheld at all levels of the company.

Impact, risk and opportunity management

Disclosure Requirement G1-1- Business conduct policies and corporate culture

Business conduct policies

As a global cybersecurity leader, Bitdefender consistently upholds the highest standards in business conduct, emphasizing its commitment to lawful and ethical operations worldwide. Our rigorous policies guide Bitdefender's corporate actions, rooted in its comprehensive Anti-Corruption Policy and Code of Business Conduct.

The Code of Business Conduct establishes the ethical foundation within which all employees and partners operate, setting clear expectations for integrity and professionalism to ensure that every business decision aligns with ethical standards. This document steers Bitdefender's interactions with stakeholders and shapes its strategies for risk management, ethical decision-making, and corporate governance.

Furthermore, the Anti-Corruption Policy articulates Bitdefender's zero-tolerance approach to bribery and corrupt practices, aligning with significant legal frameworks such as the U.S. Foreign Corrupt Practices Act and the UK Bribery Act. It outlines proactive steps taken to deter corruption, including regular risk evaluations, and stresses the importance of transparency and accountability, requiring compliance from all employees and associates.

Together, these policies reflect Bitdefender's steadfast commitment to fostering a culture of integrity and compliance. They provide not only a safeguard against legal and reputational risks but also play a vital role in enhancing stakeholder trust and ensuring long-term sustainability. Bitdefender's comprehensive ethical framework supports its strategic goals by promoting fair competition and corruption-free business practices.

Bitdefender is dedicated to maintaining a good reputation in all the markets in which it operates and practices fair competition. The company does not do business in countries on sanctions lists, and complies with EU, US and UN decisions. An internal process evaluates contracts prior to signing to ensure we avoid business relations with sanctioned entities. Bitdefender's Code of Business Conduct, approved by the CEO, represents the company's ethical framework and commitment to anti-corruption, integrity, and fair competition, being developed on six main pillars:

The six pillars of Bitdefender's Code of Business Conduct					
Build Trust and Credibility	Business done with Integrity and Responsibility	Safe Environment for our Employees	Set Metrics and Report Results Accurately	Media Inquiries	Do the Right Thing

The Code of Business Conduct underscores the significance of trustworthiness, innovation, expertise, responsibility, customer centricity, and appreciating diverse perspectives as fundamental values of Bitdefender. It provides detailed guidance on the conduct expected from every employee. The Code includes sections on legal compliance, anti-corruption initiatives, conflicts of interest, gifts, business courtesies, and competitive practices.

Applicable to all employees and officers within Bitdefender, the Code of Business Conduct directs their behavior towards adhering to legal and ethical business practices. Our commitment encompasses the principles outlined by the OECD, the U.S. Foreign Corrupt Practices Act (FCPA), the UK Bribery Act, and the UN Guiding Principles on Business and Human Rights, highlighting Bitdefender's dedication to international legal standards. This approach considers various stakeholders, including employees, customers, and partners, by emphasizing fairness, transparency, and respect for human rights. Bitdefender ensures that all employees have access to the Code, permanently available via the Intranet, to familiarize them with the company's ethical standards and expected conduct. Additionally, the Code is communicated during the onboarding process.

The Code of Business Conduct plays an essential role in Bitdefender's sustainability and governance endeavors, ensuring business practices not only comply with legal requirements but also embody high ethical standards that uphold the company's integrity and reputation within the cybersecurity sector.

Monitoring Compliance and Disciplinary Action

Bitdefender has established mechanisms to identify, report, and investigate concerns related to unlawful behavior or actions that contradict Bitdefender's code of conduct and similar internal rules. These mechanisms involve both internal and external stakeholders in the reporting process.

Under the supervision of the board of directors or a designated committee, the company's management regularly takes steps to ensure compliance with the code of conduct. This includes monitoring adherence to the code, enforcing disciplinary actions for violations, and when necessary, reporting offenders to relevant authorities.

Disciplinary actions for breaches of the code are at the discretion of the board of directors and may range from counseling and warnings to probation, suspension (with or without pay), demotion, reduced salary, termination of employment, or restitution. All violations are assessed through a fair process, where accused individuals are given the chance to present their side of the story before any disciplinary action is decided.

Management is also responsible for periodically reporting to the board of directors or authorized committees about these compliance activities, including reports on alleged violations and the subsequent actions taken. This ensures transparency and accountability in maintaining the company's ethical standards.

Whistleblower protection

Bitdefender has implemented a Whistleblowing Procedure as part of its commitment to maintain the highest standards of ethical and legal conduct across its operations. This vital framework aims to enhance transparency and promote sound governance by offering explicit guidelines for reporting and addressing concerns regarding potential misconduct. The procedure ensures that all reports submitted through designated whistleblowing channels are handled with strict confidentiality and care. The procedure is reviewed on an annual basis, with the most recent review conducted on 19 September 2024.

Multiple channels are available for whistleblowing, allowing concerns to be raised anonymously by employees and external parties alike:

- **Email**: ethics@bitdefender.com, compliance@bitdefender.com and hr@bitdefender.com
- **Online form**: https://www.bitdefender.com/en-us/site/view/legal-ethical-compliance

The company reinforces awareness and appropriate use of whistleblowing channels by integrating them into mandatory annual employee training programs. These channels are specifically covered in the **Anti-Corruption** and **Business Code of Conduct** trainings, which all employees are required to complete each year. This approach ensures that staff are well-informed about how to raise concerns and reinforces the company's commitment to ethical conduct and transparency.

The Anti-Corruption Compliance function, situated within the Fraud Prevention and Office Security Department, plays a pivotal role in overseeing the thorough examination of every report, safeguarding the whistleblower's anonymity. This reflects Bitdefender's commitment to fostering a safe environment where ethical issues can be reported without fear of retaliation, aligning all business activities with its core values and legal duties. The policy is applicable to all Bitdefender employees, contractors, and associated individuals globally, addressing a variety of concerns that could affect the company's integrity and compliance, from fraud and corruption to other legal or regulatory infringements.

The implementation of this policy is managed by the Anti-Corruption Compliance function, which is responsible for initially assessing the reports, maintaining documentation, and determining investigative actions. Their activities receive support from higher governance structures, including regular reviews and reports to the CEO. The policy aims to protect the company and its stakeholders — Including employees, partners, and shareholders—from risks associated with corruption and unethical practices. It offers a secure and confidential method for stakeholders to report concerns, thereby contributing to a transparent and accountable workplace.

The Whistleblowing Procedure and Whistleblowing Investigation Procedure are accessible via the intranet, ensuring that all relevant stakeholders and responsible personnel are informed about how to access, understand, and comply with the procedures. This comprehensive strategy underscores Bitdefender's dedication to cultivating a business environment rooted in ethics, enabling concerns to be raised without fear of retaliatory actions, and promoting a culture of openness and compliance.

Employees seeking advice on implementing Bitdefender's policies and practices for responsible business conduct, including due diligence and anti-money laundering, can request support via a broader spectrum of communication channels: ethics@bitdefender.com, legal@bitdefender.com, compliance@bitdefender.com, privacy@bitdefender.com, dpo@bitdefender.com and Customer support channels.

Regarding the organization's business conduct, stakeholders can raise concerns via the whistleblowing channel available at the following link: https://www.bitdefender.com/site/view/legal-ethical-compliance.html

Training on business conduct

Bitdefender has established a structured and mandatory training framework on business conduct, applicable to all employees. As part of the onboarding process, new employees are required to complete training on the Code of Business Conduct within 21 days of their start date.

In addition, all employees must undergo annual refresher training, scheduled one year from the completion of their previous session, to ensure continued awareness and compliance. These training modules are delivered through the company's Human Capital Management System, which also manages automated notifications and deadlines.

Completion of mandatory training is closely monitored, and failure to comply may result in the temporary suspension of system access. Beyond the initial onboarding, employees are periodically assigned additional training throughout the year, reinforcing the company's commitment to upholding high standards of ethical conduct across the organization.

Functions-at-risk

In line with Bitdefender's risk management framework, teams identified through our internal risk assessment as presenting a heightened risk for fraudulent activities (including anti-bribery risks) are actively involved in our annual fraud risk assessment workshops. These teams typically include employees in management positions or roles with decision-making authority. During these workshops, relevant controls are identified and evaluated, the net risk position is assessed against our established risk appetite, and additional treatment actions are applied where necessary to ensure alignment with our risk tolerance and compliance standards.

Disclosure Requirement G1-2 - Management of relationships with suppliers

Bitdefender is committed to fostering strong, collaborative relationships with its suppliers, recognizing that a resilient and sustainable supply chain is vital to delivering high-quality cybersecurity solutions.

Our company does not have a formal policy for late payments. However, we maintain a strong financial position and high creditworthiness, ensuring that our suppliers are always paid on time. Even during the challenges of the pandemic, we remained committed to timely payments, particularly supporting small and medium-sized enterprises (SMEs). This reliability reflects our dedication to financial responsibility and strong business relationships.

Bitdefender suppliers are required to acknowledge the adoption and use of OECD Guidelines for Multinational Enterprises for both internal use and within their extended supply chain, in order to provide goods or services to Bitdefender.

Starting in 2026, Bitdefender will integrate social and environmental criteria into its supplier selection process, aligning with the European Sustainability Reporting Standards (ESRS). This initiative reflects the company's commitment to responsible sourcing, ensuring that its suppliers adhere to ethical labor practices, environmental sustainability, and human rights standards. By incorporating these criteria, Bitdefender aims to mitigate risks associated with its supply chain, promote sustainability, and strengthen its contribution to a more responsible and resilient business ecosystem.

For all marketing-related expenditures at a global level, Bitdefender utilizes a dedicated procurement platform where approval workflows are predefined, budget limits are strictly verified, and cost centers are assigned. Only expenditures within the allocated budget receive approval, ensuring financial control and responsible spending. Once approved, suppliers proceed to the contract management platform, where agreements are signed electronically, streamlining the process while ensuring compliance with company policies and legal requirements.

For other types of expenses, Bitdefender conducts a quick vendor assessment before entering into a contractual agreement. This assessment ensures that suppliers meet the company's operational and compliance standards. Additionally, financial data related to these vendors is integrated into Bitdefender's Enterprise Resource Planning (ERP) system to enhance transparency and informed decision-making.

By embedding these procurement practices into its operations, Bitdefender upholds principles of fairness, accountability, and financial responsibility, fostering ethical business relationships and a resilient supply chain.

Disclosure Requirement G1-3 - Prevention and detection of corruption and bribery

Bitdefender's Anti-Corruption Policy is established to ensure full compliance with international anti-corruption legislation, including the U.S. Foreign Corrupt Practices Act (FCPA), the UK Bribery Act, and other applicable laws. The policy strictly prohibits bribery and the offering or acceptance of any improper advantage. It provides comprehensive guidance on avoiding corrupt practices, outlines clear compliance procedures, and sets standards for managing gifts, hospitality, political contributions, and charitable donations.

This policy applies uniformly to all directors, officers, and employees across Bitdefender's global operations. It also extends to third parties acting on behalf of Bitdefender—such as agents, consultants, and suppliers—who are equally expected to adhere to these standards. Bitdefender places a strong emphasis on ensuring that both internal and external stakeholders comply with its anti-corruption framework.

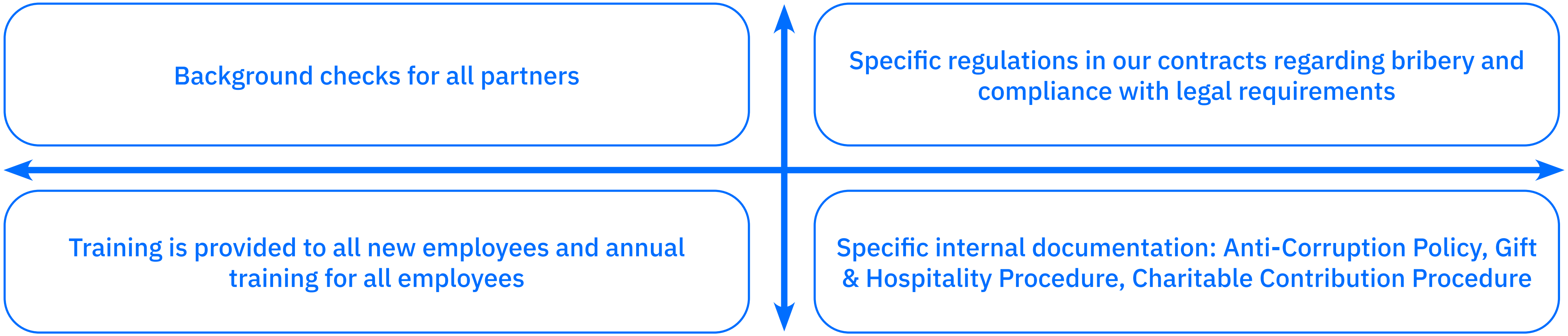
Responsibility for implementing and overseeing this policy lies with the Anti-Corruption Compliance Officer, who also serves as the Director of Fraud Prevention and Office Security. This role includes monitoring compliance, addressing reported violations, and updating the policy to reflect evolving global anti-corruption standards.

Bitdefender's Anti-Corruption Policy is aligned with internationally recognized compliance practices and incorporates the requirements of key legislative frameworks such as the FCPA and the UK Bribery Act. The policy is made accessible to all relevant stakeholders, ensuring that employees and associated third parties are well-informed of their obligations and Bitdefender's ethical principles.

To support effective implementation, employees receive regular training on anti-corruption practices, including video modules and in-depth case studies. It is essential that employees act with integrity and avoid any conflicts of interest that could influence their professional decisions. As part of Bitdefender's ongoing anti-corruption efforts, all employees are required to sign an annual Declaration of Interest, reaffirming their commitment to ethical conduct. The full Anti-Corruption Policy and related procedures are readily available to all staff via Bitdefender intranet.

Overall, the Anti-Corruption Policy is part of Bitdefender's broader strategy to uphold integrity and ethical conduct in all areas of operation, ensuring that all business dealings are transparent and fair.

Bitdefender has several controls in place to prevent and detect incidents of corruption and bribery:



Background checks for all partners

Specific regulations in our contracts regarding bribery and compliance with legal requirements

Training is provided to all new employees and annual training for all employees

Specific internal documentation: Anti-Corruption Policy, Gift & Hospitality Procedure, Charitable Contribution Procedure

Bitdefender has a dedicated compliance team responsible for conducting background checks and reporting any instances of non-compliance to the Legal Team. In line with our internal risk assessment, all employees in risk-related functions are required to complete mandatory annual online training.

Metrics and targets

Disclosure Requirement G1-4 - Incidents of corruption or bribery

Disclosure Requirement G1-5 - Political influence and lobbying activities

Bitdefender is committed to maintaining the highest standards of ethical conduct and integrity in its operations worldwide. The Anti-Corruption Policy outlines explicit sanctions for any violations or breaches, ensuring stringent enforcement to uphold compliance and ethical standards.

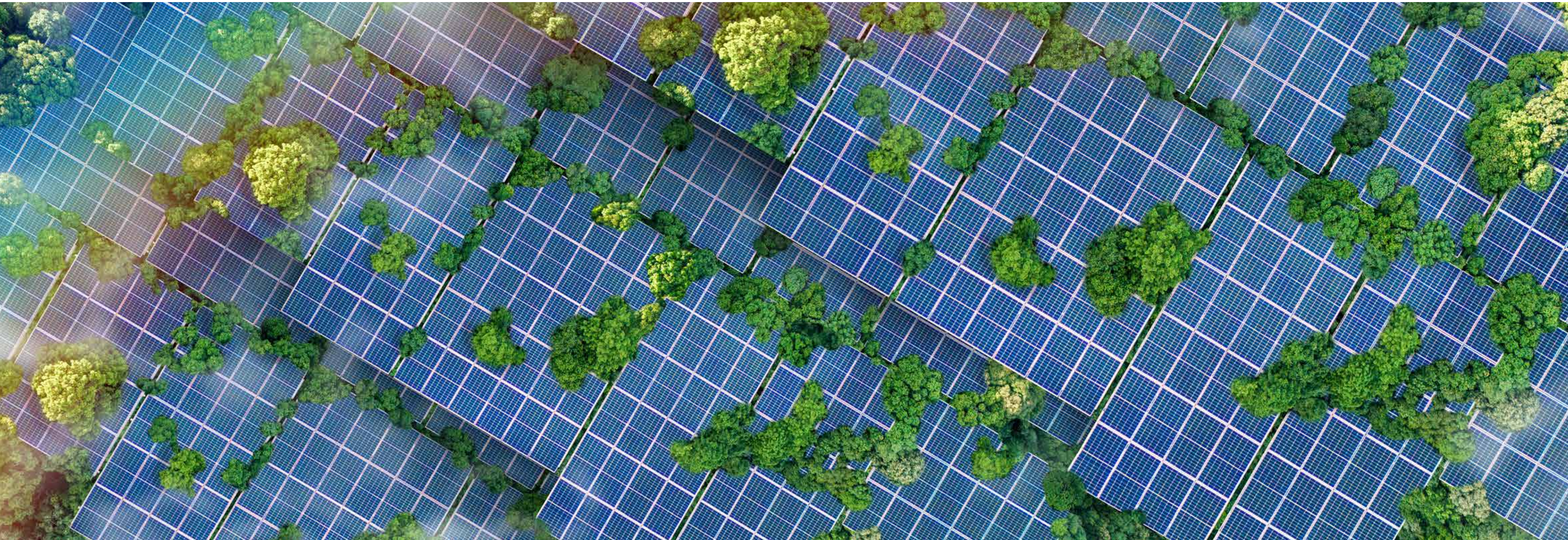
The sanctions for non-compliance may range from appropriate disciplinary actions, such as demotion, reassignment, additional training, probation, or suspension, to the most severe measure of termination of employment. By defining clear penalties, Bitdefender demonstrates its zero-tolerance stance towards corruption and sets expectations for the conduct of all employees.

During the reporting period, Bitdefender proudly reports no incidents of corruption or bribery. The company has not faced any convictions or fines related to the violation of anti-corruption and anti-bribery laws, showcasing the effectiveness of its policies and the ethical commitment of its workforce. Additionally, Bitdefender maintained transparency in its political engagement by refraining from making any political contributions, ensuring that its operations remain impartial and focused on business integrity.

Disclosure Requirement G1-6 - Payment practices

Bitdefender’s commitment to responsible financial management is reflected in its efficient payment practices. On average, the company processes invoices within a timeframe of 1 to 30 days, commencing from the date the contractual or statutory term begins. The adherence to prompt payment schedules helps fortify relationships with partners and contributes to smoother operations by ensuring that all parties can rely on timely funds. Bitdefender recognizes the importance of this aspect of business conduct and continually strives to optimize its invoicing processes for maximum efficiency.

Throughout the reporting period, Bitdefender’s adherence to its payment commitments has resulted in a record free from outstanding legal proceedings related to late payments. This track record demonstrates the company’s proactive approach and its diligence in honoring financial obligations in a timely manner.



Bitdefender®

Cybersecurity and Data protection

In today’s digital era, cybersecurity is crucial not just for operational integrity, but for achieving sustainability goals. It has evolved from a technical issue to a core aspect of corporate responsibility and sustainable business practices. Bitdefender is dedicated to transforming the cybersecurity landscape by offering cutting-edge solutions to government bodies, large enterprises, SMBs, and individuals across over 170 countries. Prioritizing customer privacy, Bitdefender employs rigorous measures to secure client data and uphold confidentiality, mitigating the risk of breaches.

In this chapter

Cybersecurity and Data Protection

Cybersecurity

In our globalized world, cybersecurity has become a crucial element underpinning both operational integrity and wider sustainability objectives. In the digital age, it plays a vital role in sustaining any business. The link between a solid cybersecurity infrastructure and enduring business sustainability has never been more pronounced. Safeguarding against cyber threats has transcended technical concerns, evolving into a vital aspect of corporate responsibility and sustainable business strategies.

Out of all sustainability factors, cybersecurity, or its lack thereof, exerts a significant impact on social issues. Poor cybersecurity creates vulnerabilities within various economic sectors. Recent events show that even minor security gaps can greatly affect essential areas like healthcare, transportation, and financial markets, ultimately impacting individuals personally. Enhancing cybersecurity not only protects businesses but also improves societal wellbeing, trust, and security as a whole. Investing in strong cybersecurity practices contributes to a more stable and secure environment for all, highlighting cybersecurity as a key element of broader social and economic sustainability.

As digital threats become more complex and widespread, we are committed to enhancing cybersecurity for both our customers and society. This commitment reflects our dedication to fostering sustainability through supporting companies in building long-term resilience. The evolving threat landscape presents businesses with unprecedented challenges that can jeopardize their operations, financial health, and reputation. The increasing complexity of cyber threats highlights the need for effective cybersecurity strategies. With cybercriminals constantly evolving, organizations must not only defend against these threats but also align these defenses with sustainable growth. Bitdefender is focused on providing advanced, proactive solutions to strengthen our clients' defenses against a variety of cyber threats. Bitdefender steps forward with solutions that not only address immediate threats but also contribute to building resilience and sustainability within our clients' operations. Our advanced threat detection and response services help companies manage risks that could otherwise disrupt their operations and compromise their sustainability objectives. For example, our Managed Detection and Response (MDR) services offer continuous monitoring and swift response, ensuring businesses can sustain operational continuity even amidst sophisticated cyberattacks.

Additionally, we concentrate on creating advanced technologies that predict and counteract new threats, like ransomware and assaults on cloud infrastructure. This proactive strategy not only safeguards our clients' data but also empowers them to innovate and grow sustainably, without the fear of crippling cyber incidents.

Our GravityZone platform, renowned for its comprehensive security capabilities, plays a pivotal role in safeguarding digital infrastructures.

Utilizing advanced threat detection mechanisms, machine learning algorithms, and behavioral analytics, GravityZone equips businesses to outpace evolving cyber threats. This strategic approach not only mitigates immediate dangers but also supports long-term sustainability by maintaining business continuity and reducing downtime.

Digital transformation is a crucial driver of sustainability, enabling businesses to function more efficiently and decrease their environmental impact. As organizations navigate digital transformation, they encounter new challenges linked to an expanding attack surface. Bitdefender is committed to overcoming these challenges by providing state-of-the-art solutions that secure digital environments. Our solutions are crafted to protect the intricate ecosystems arising from digital transformation, allowing our clients to pursue innovative strategies without sacrificing security. Our cloud security offerings are tailored to guard against threats targeting cloud infrastructures, empowering businesses to confidently utilize cloud technologies while safeguarding their data and operations.

The widespread adoption of Internet of Things (IoT) devices presents another crucial focus area. Often deployed with inadequate security measures, IoT devices can serve as gateways for cybercriminals. Bitdefender's partnership with hardware manufacturers to bolster IoT device security underscores our commitment to supporting digital transformation while maintaining network security. By securing these devices, we prevent them from becoming vulnerabilities that cybercriminals can exploit, thereby safeguarding the integrity of our clients' networks and supporting their sustainable growth. Through these efforts, we help businesses effectively manage their cybersecurity risks, contributing to their overall sustainability objectives.

Bitdefender's commitment to cybersecurity goes beyond shielding individual businesses. We aim to cultivate a secure digital environment for all users and communities. Our offering of free security tools for personal devices reflects our broader responsibility to enhance cybersecurity society-wide. By providing accessible protection, we contribute to reducing the overall risk of cyber threats, bolstering a safer online environment for both individuals and organizations.

Cybersecurity is increasingly integral to corporate social responsibility (CSR) and environmental, social, and governance (ESG) frameworks. It is crucial for data protection, business continuity, and ethical digital practices. At Bitdefender, we embed cybersecurity into our ESG strategy by prioritizing data security, ethical technology use, and global security initiatives.

Our commitment to cybersecurity innovation aligns with promoting sustainable development and responsible business practices. By tackling cybersecurity challenges, we enhance a secure and resilient digital economy, reinforcing our dedication to sustainable practices and safeguarding digital assets.

The future of cybersecurity offers challenges and opportunities. Bitdefender remains at the forefront, evolving solutions to address threats and support clients' sustainability goals. Our focus on research and development keeps us agile in navigating the threat landscape.

We aim to advance cybersecurity offerings while fostering security awareness and resilience. By educating clients and the community on cybersecurity best practices, we empower effective self-protection. This educational focus complements our technological advancement.

Innovation drives Bitdefender's cybersecurity approach. Our research in AI and machine learning boosts threat detection and response, staying ahead of cybercriminals to offer top-tier protection. For instance, our SafePay technology offers a secure browsing environment for online transactions, shielding users from threats like phishing and malware. By continually evolving our technology, we ensure that our clients have access to the latest innovations in cybersecurity, supporting their ongoing efforts to maintain a secure digital presence.

Collaboration is crucial for tackling the complex and evolving challenges of cybersecurity. Bitdefender actively partners with industry leaders, hardware manufacturers, and stakeholders to strengthen the security of digital ecosystems. These partnerships allow us to create comprehensive solutions addressing various cybersecurity issues, enhancing the overall resilience of the digital landscape.

Our work with hardware manufacturers to secure IoT devices exemplifies our collaboration to boost cybersecurity. By incorporating security measures into hardware design, we help mitigate vulnerabilities that cybercriminals could exploit. This cooperative approach aids our clients in effectively managing cybersecurity risks, promoting a more secure and sustainable digital environment.

Cultivating a culture of cybersecurity awareness is central to Bitdefender's strategy. We believe education and awareness are vital for empowering individuals and organizations against cyber threats. Our initiatives to educate users on cybersecurity best practices, such as strong passwords and secure online conduct, are key to our commitment to enhancing digital security.

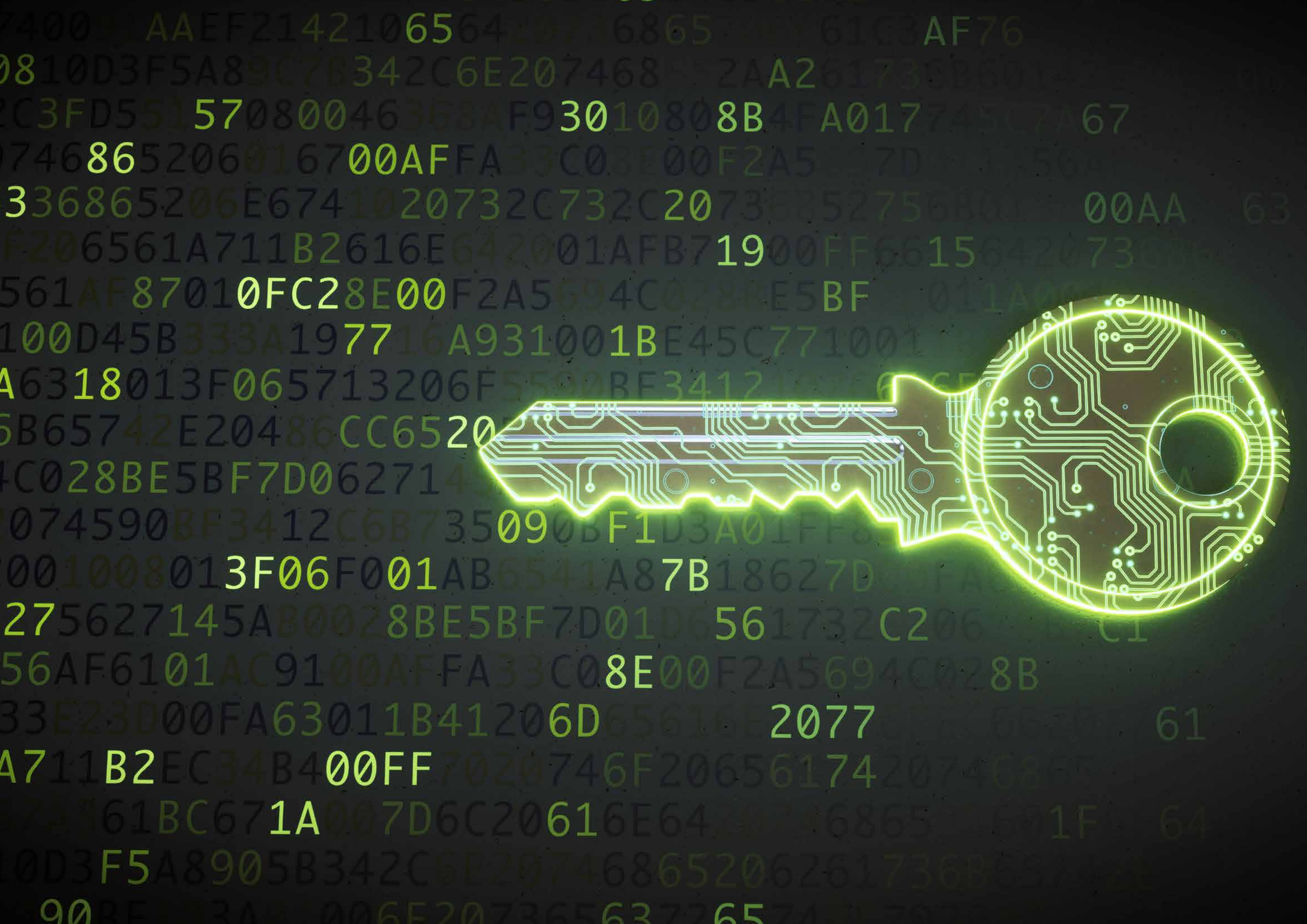
Through public awareness campaigns and educational programs, we aim to elevate understanding of cybersecurity risks and encourage responsible digital practices. By fostering cybersecurity awareness, we contribute to a safer and more resilient digital ecosystem, aligning with our broader sustainability goals.

Efficient incident response and recovery are essential elements of a strong cybersecurity strategy. Bitdefender's MDR services offer advanced incident response capabilities to swiftly address and contain security incidents. With expert support available around the clock, we ensure businesses effectively manage and recover from cyber incidents.

> Our dedication to incident response and recovery reflects our commitment to enhancing the long-term resilience of our clients. By delivering prompt and effective response services, we assist businesses in reducing the impact of cyber incidents, thereby ensuring continuous operations. This emphasis on recovery not only fosters the overall sustainability of our clients but also underscores our devotion to safeguarding their digital assets.

Bitdefender's cybersecurity strategy is closely linked with our dedication to sustainability. By offering advanced protection, encouraging digital transformation, and participating in global security initiatives, we significantly contribute to nurturing a secure and sustainable digital future. Our continual endeavors in innovation, education, and collaboration promote a more resilient and secure digital landscape, aligning with our broader aim of sustainable development.

As we envision the future, Bitdefender remains committed to enhancing cybersecurity practices and fostering a culture of security awareness. Our pledge to innovation, collaboration, and education will persist in driving our efforts to safeguard digital assets and uphold sustainable business practices. Through these initiatives, we strive to contribute to a more secure and resilient digital economy, benefiting businesses, individuals, and communities worldwide.



Data protection

Bitdefender partners with a diverse range of clients, including governmental bodies, multinational corporations, small and medium-sized enterprises, and individual users spanning over 170 countries. The company is dedicated to transforming the cybersecurity field by offering cutting-edge products and services that excel in efficiency, performance, and user experience, while ensuring seamless integration. Prioritizing customer privacy, Bitdefender implements stringent measures to safeguard the security and confidentiality of client data, ensuring the prevention of breaches.

The Bitdefender Code of Business Conduct highlights the company's commitment to data protection among other ethical guidelines. This document details how Bitdefender globally safeguards the personal information of its employees, customers, and business partners. Adhering to Privacy Principles, the policy ensures that the collection, processing, and retention of personal information are conducted legally, fairly, transparently, and securely. Specific pledges include minimizing data collection, ensuring data accuracy, limiting retention to necessary durations, and maintaining robust security and confidentiality.

Furthermore, the policy outlines procedures for handling personal data, emphasizing the lawful, fair, and transparent collection and processing of data. It requires that personal information be retained only as necessary for specific legitimate purposes. Additionally, it specifies stringent security measures to protect personal data against unauthorized access or disclosure.

Bitdefender guarantees that all personal data handling complies with its ethical standards and privacy commitments, which are vital for sustaining trust and credibility in its cybersecurity endeavors. The detailed strategy detailed in the Code of Business Conduct showcases Bitdefender's devotion to maintaining exemplary data protection and privacy standards throughout its operations.

In 2024, Bitdefender experienced a decrease in data protection complaints related to individual customers, reduced from 10 cases in 2023 to **5 cases in 2024**. These incidents were primarily related to human errors where customer data, such as email addresses, were inadvertently disclosed to unintended recipients. Importantly, all 5 cases were categorized similarly to the incident reported in 2023, which involved the erroneous sharing of a customer's email or other data with another client. These incidents were flagged internally, communicated to the affected customers, and corrective measures were taken to prevent future occurrences. Despite these incidents, there were no complaints from regulatory bodies, nor were there any identified leaks, thefts, or losses of customer data reported during this period. The total number of data subject requests also saw fluctuations, decreasing from 4,254 in 2023 to **4,118 in 2024**.

Bitdefender®

Global Leader
In Cybersecurity

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

Corporate Headquarters
Registered address
Orhideea Towers, 15A Orhideelor Road, 6th District,
Bucharest 060071, Romania
T: +40 21 4412452
F: +40 21 4412453

Bitdefender Holding B.V.
Registered address
174 Maanweg, Building C, 4th floor,
2516AB The Hague, The Netherlands

office@bitdefender.com

Bitdefender-Corporate-SustainabilityStatement2024-brand232
CD-10/06/25 • MD-October 23, 2025 12:03 PM