JUNE 2026

Visma Code of Conduct

VISMA

Introduction

by Merete Hverven, CEO of Visma

A company's achievements are only as great as the strength of its people. Visma has amazing people, and it is through their ideas, teamwork, and dedication that Visma has become the leading global software company it is today.

Whether you're a new employee or have been in Visma for 20 years, your decisions will have a significant impact on our company. We wouldn't have it any other way: when people experience trust and freedom – to experiment, learn, grow, and pursue meaning – everyone benefits.

The understanding that thriving employees lead to a more successful company has been fundamental to Visma since its founding. Our core values Entrepreneurial, Responsible, Dedicated, and Inclusive form the basis of our internal and external relationships.

They are vital not only to how we do our jobs, but also how we are perceived by our customers, our partners, and society.

The Visma Code of Conduct is an expression of the responsibility that you, as a Visma employee, carry. It serves as a guide for how our core values translate into our attitudes and behaviour. In short, it is a blueprint reminding us to always act ethically, lawfully and mindfully of what is best for our customers, our coworkers and society as a whole. The Code of Conduct is also a living document that should evolve based on continuous feedback and dialogue. It is therefore important that you feel comfortable bringing up any questions or input you have directly with your closest leader. That way, we can ensure together that the Code of Conduct is as meaningful and effective as it can be. **Welcome to Visma!**

Merete Hverven
CEO of Visma



Table of contents

Introduction 02

About the Code of Conduct 04

People 05

- A safe and healthy work environment 06
- Diversity, equality & inclusion 07
- A harassment-free environment 08
- Avoiding drugs and alcohol 09

A responsible and sustainable business 10

- Human rights 11
- Environmental responsibility 12
- Supplier relationship 13
- Anti-corruption 14
- Conflicts of interest 15
- Gifts and hospitality 16
- Anti-fraud and accurate records 17
- Anti-money laundering 18
- Competition and market regulations 19
- Sanctions and export control 20
- Responsible use of AI 21

Safeguarding assets 22

- Companies' assets 23
- Confidential information 24
- Data protection 26
- Cost control and tax practices 27
- Representing Visma in public 28

Speak up and make a difference 29

- Contact us 30

About the Code of Conduct

The scope
The Visma code of conduct outlines minimum behavioral standards for all employees in Visma.

The Code covers 4 main topics:

- **People**
- **Responsible and sustainable business**
- **Safeguarding Visma's assets**
- **Whistleblowing**

This code of conduct forms a foundational guide, supported by Visma Group policies.
Visma companies may have supplemental policies that comply with this Code.
All employees across the Visma Group are responsible for upholding these principles in their daily work to ensure ethical and compliant conduct.
Please read carefully and bear in mind that each of us has a responsibility to incorporate these principles and values into our everyday work. Acting against the principles may lead to disciplinary actions or, if severe, termination of employment.

Visma's suppliers
Visma expects its suppliers and business partners to uphold the same high ethical and legal standards we do.
When engaging with new suppliers, ensure they align with these principles by following Visma Vendor Management framework. For more details on our expectations, please refer to the Visma Supplier Code of Conduct.

Reporting a breach
If you detect or suspect a breach of this Code of conduct, report it immediately to your leader or anonymously through our Whistleblowing Channel. Visma prohibits all retaliation against employees who report or participate in an investigation into a possible breach.

Code of Conduct responsibility
The Visma AS Board has approved this Code, and Visma Group Wide Services is responsible for its regular review.

Questions and concerns
For any questions or concerns about this Code of conduct, please contact your leader and/or People/Human Resources representative, or your Managing Director.



Mission

Visma's goal is to empower SMBs to thrive and local governments to serve by making business administration effortlessly simple.



Values

We are entrepreneurial
We are responsible
We are dedicated
We are inclusive.

01

People

Our collective success relies on the strength of our people. We are committed to fostering an environment where every individual feels safe, respected, and empowered.

This section outlines our core values and shared responsibilities for creating a culture of diversity, inclusion, and well-being across all our companies.

- A safe and healthy work environment
- Diversity, equality & inclusion
- A harassment-free environment
- Avoiding drugs and alcohol



A safe and healthy work environment

Our goal is to be the most inspiring and engaging place to work - a place where all of our employees can succeed, thrive, and realise their full potential. To make that happen, we need a safe and healthy environment where everyone feels comfortable sharing their opinions, trying new things, and being themselves.

We all have a part to play in creating an inclusive and respectful workplace. Please get involved with our safety and environmental efforts and help us create a safe and healthy work environment for everyone. If you notice anything that could be a risk to someone's health or safety (such as an unsafe situation, a faulty installation, or any other risk), please let your manager or safety representative know right away.

Employee engagement survey (EES)

Having engaged people is a key driver of our business. We measure employee engagement frequently through monthly or bi-monthly engagement surveys, with the purpose of providing our employees with a channel to give their anonymous feedback.

The survey results provide valuable input on what is working well and what we can improve, and by participating, you contribute to further developing your and your colleagues' work environment, collaboration and general engagement.



We value diversity

Our strength lies in our differences. We build relevant, high-quality products by bringing together employees from diverse backgrounds, experiences, and perspectives. This diversity allows us to better understand and serve our customers. To support this, we use structured recruitment processes, highlight diverse role models, and offer various training and flexible work options.

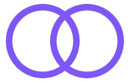
We ask you to contribute by being open-minded and welcoming of others' perspectives. If you want to learn more, we advise you to join our DEI community on Visma Space. For more information on how Visma uses diversity to develop a healthy work culture, view our web pages and the Visma Sustainability Policy.



We value equality

We are committed to a workplace where your opportunities for growth and advancement are based on your talent and hard work - not your gender, age, ethnicity, or any other personal characteristic.

We work hard to eliminate all forms of discrimination and harassment and to create a culture where everyone is treated with respect. By treating each other with dignity, you contribute to build a truly equitable workplace.



We value inclusion

An inclusive culture is essential for us to truly benefit from our diversity. Inclusion is what makes us feel safe enough to bring our whole selves to work and share our opinions freely.

We want every person at Visma to feel valued and like they belong. Our leaders work to create an inclusive environment where everyone can fully engage with their work and share their ideas without judgment.

A harassment-free environment

Harassment in any form will not be tolerated at Visma. This includes but is not limited to: offensive comments, inappropriate behaviour in any way, bullying, intimidation, or anything that creates a hostile or uncomfortable environment for others.

We are committed to providing a harassment-free and inclusive workplace for everyone, regardless of gender, gender identity and expression, sexual orientation, disability, physical appearance, body size, race, religion, or any other characteristic. If you experience or witness harassment, please report it to your nearest leader or local HR.

Recognizing harassment in the workplace:

- Pay attention to any behaviour that makes you feel uncomfortable, intimidated or targeted based on your protected characteristics.
- Be aware of subtle forms of harassment, such as exclusion, microaggressions or persistent and unwelcome comments.
- Trust your instincts. If something feels wrong or inappropriate, it's important to address it.

What to do in cases of harassment:

- Speak up: If you experience or witness harassment, consider addressing the issue directly with the person involved if you feel safe to do so.
- Report the harassment to your leader, local HR or use our Whistleblowing channel where you can report anonymously.
- Seek support: Don't hesitate to seek support from colleagues, local HR, or other trusted resources within the organisation. You are not alone, and support is available.

Remember, creating a safe and respectful workplace is everyone's responsibility. By being vigilant, speaking out against harassment, and supporting one another, we foster a culture of respect and equality for all.



Avoiding drugs and alcohol

Visma employees' health and safety retain a top priority. We want to create a safe working environment for all our employees.

Alcohol must be avoided if the use leads to impaired performance, health issues, inappropriate behaviour, missing work engagements or deadlines, danger to the safety of others, or violations of the law. Visma practises a zero tolerance policy for illegal substances in any form.

Please remember, even when you are outside of our offices, that you are still expected to practise good judgement and will be responsible if your behaviour impacts performance, our company brand(s) or your working relationships. Please bear in mind that you are still regarded as an employee at social gatherings, business travels, and dinners sponsored by the employer. As such, it is expected that you conform to our guidelines also in these settings.

Visma has resources available to support and assist employees struggling with alcohol- or substance abuse. If you want to learn more, contact your leader or local HR.

02

A responsible and sustainable business

A core Visma value is to be responsible, which means operating with integrity and being compliant.

All employees must adhere to local legislation; while specific requirements vary by country, fundamental universal legal standards apply.

Our Visma group policies provide a framework for governance and compliance. They are approved by Visma's CRO and CFO and are accessible to all employees here. If uncertain about a legal requirement, consult your local legal counsel or the Visma Group Legal & Compliance team before acting.

- Human rights
- Environmental responsibility
- Supplier relationship
- Anti-corruption
- Conflicts of interest
- Gifts and hospitality
- Anti-fraud and accurate records
- Anti-money laundering
- Competition and market regulations
- Sanctions and export control
- Responsible use of AI



Human rights

Visma does not tolerate any human rights violations and is dedicated to ensuring it does not cause or contribute to adverse human rights impacts within the company, its supply chain, or among its suppliers, partners, and other stakeholders. Our commitment to human rights is based on the Universal Declaration of Human Rights and the core principles of the International Labour Organisation's (ILO) Declaration on Fundamental Principles and Rights at Work.

Visma adheres to the five fundamental principles as defined by the ILO:

- Promoting freedom of association and the right to collective bargaining.
- Eliminating all forms of forced or compulsory labor and modern slavery. This means all workers are employed voluntarily and are not required to give the company any deposits, money, or personal papers.
- Prohibiting child labor. Visma and its business associates are not to employ workers below the minimum age for work or mandatory schooling as specified by local law.
- Eliminating discrimination in employment and occupation.
- Maintaining a safe and healthy working environment for all employees.

All employees are responsible for avoiding any actions that could cause or contribute to adverse human rights impacts, either directly or indirectly through Visma's business relationships. Any suspected human rights breaches within Visma or its value chain should be reported through the Visma Whistleblowing channel or regular reporting lines.

Environmental responsibility

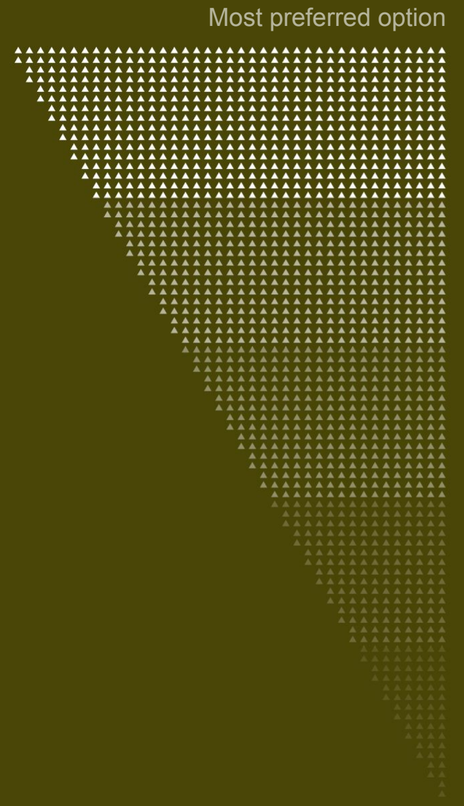
As a signatory of the UN Global Compact, Visma is committed to minimizing our environmental impact and promoting sustainable practices. All employees play a part in this.

You can learn more about Visma's environmental targets and our sustainability initiatives on our website, in the Visma Sustainability Policy and on Visma Space (for Visma employees only).

How to contribute to Visma's environmental responsibility

- Make Sustainable Decisions: Consider the environmental impact of your business choices, especially those related to procurement. See the Visma Supplier Code of Conduct for Visma's expectations of our suppliers.
- Reduce Business Travel: Prioritize video conferencing over non-essential business trips, particularly air travel. For essential travel, choose trains or buses over flights when the travel time is reasonable. All employees should follow the guidance in the Visma Travel Policy.
- Choose Sustainable Commutes: Opt for public transport, cycling, or walking for your daily commute.
- Use hardware sustainably: Reduce waste by extending the lifespan of hardware like computers and phones. As an employee, always consider whether you really need a new device. When equipment reaches its end-of-life, ensure it is properly recycled.
- Avoid Food Waste: Be mindful of food waste and consider climate-friendly, plant-based options when organizing business events.
- Consider the environmental impacts of software: Where applicable, apply sustainable software engineering principles and follow Visma's guidance on the responsible use of AI.

The waste hierarchy



Refuse
Waste prevention: waste avoided completely

Reuse/Repair
Repairing: extending life of products without other pre-processing

Recycle
Recovering materials and reprocessing them into new products

Recover
E.g. incineration with energy recovery

Dispose
Landfill incineration without energy recovery

*When dealing with natural resources and physical materials, always follow the principles of the waste hierarchy.

Supplier relationship

Visma's commitment in all supplier relationships is built on integrity, fairness, and compliance. Integrity builds trust and long-term partnerships. Fairness creates an equitable environment ensuring all suppliers have equal opportunities. Compliance ensures adherence to legal obligations, safeguards our reputation and promotes sustainable and responsible business practices.

These **key principles** are actionable guidelines, empowering our teams to make ethical and responsible decisions daily.

Your responsibility is to uphold these standards and report concerns through official channels. For more information, see the Visma Supplier Code of Conduct.

01

Zero tolerance for corruption

Absolutely no bribes, kickbacks, or improper inducements.

02

Ethical conduct

Fair treatment: Treat all suppliers objectively and without bias.
No conflicts of interest: Disclose any personal or financial ties that could influence decisions.
Gifts & entertainment: To be modest and infrequent and never to influence decisions.
Confidentiality: Protect all sensitive information.

03

Responsible procurement

Transparent processes: Fair and competitive selection of suppliers.
Contractual clarity: All engagements must have clear, written agreements.
Data security: Adhere to strict security protocols.
IP protection: Respect and protect intellectual property rights.

04

Compliance

Adhere to applicable laws and internal guidelines including Vendor management, Anti-corruption and Data protection.

Anti-corruption

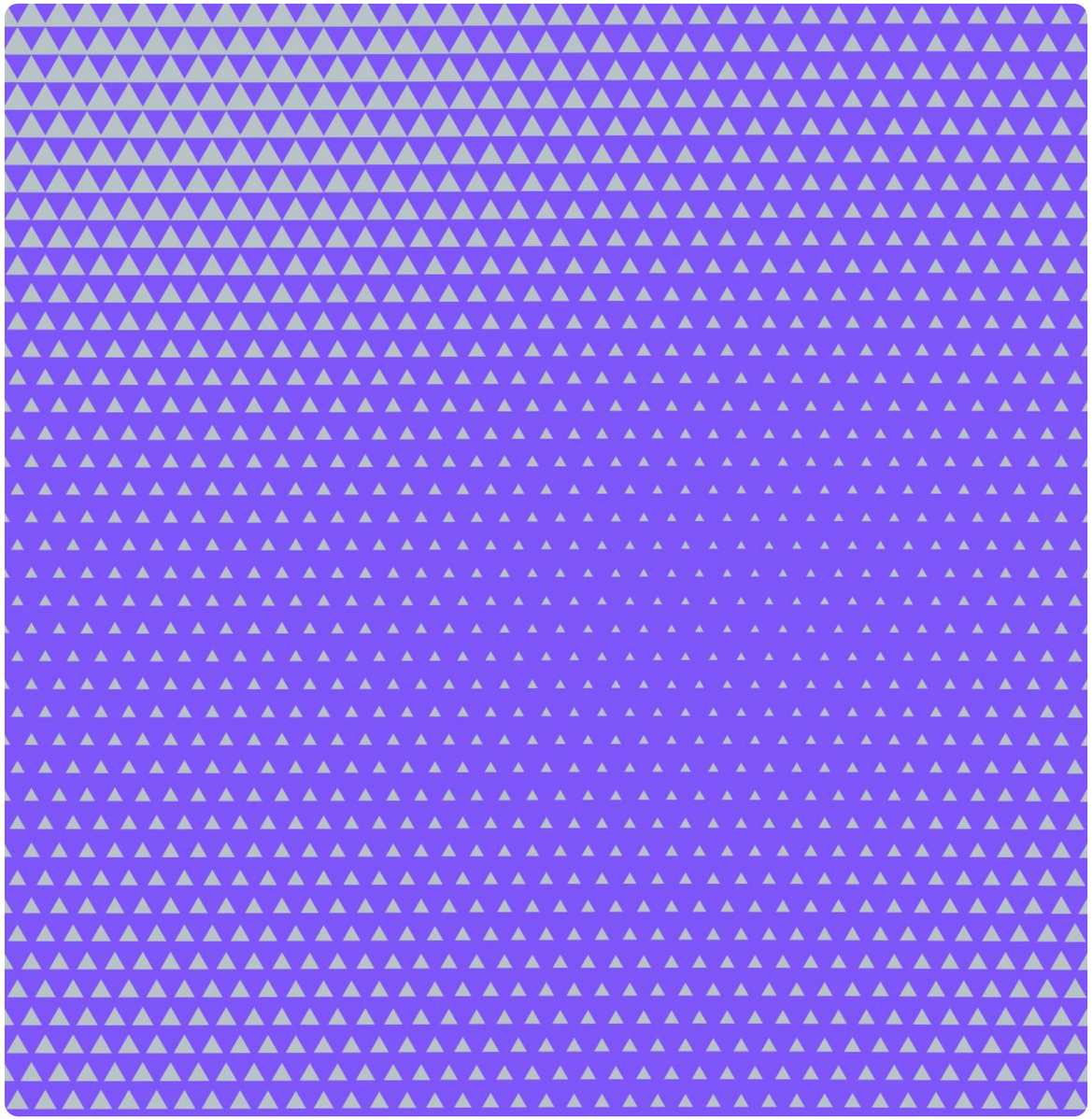
Visma has a zero-tolerance policy for all forms of corruption. Demanding, offering or accepting anything of value to improperly influence a business decision or action is corruption. Engaging in any form of corruption is illegal and causes irreparable harm to Visma's integrity and trust with customers, partners and the public.

Integrity is fundamental to our business, and every employee has a personal responsibility to uphold this standard by acting with transparency and sound judgment. As a Visma employee, you shall always act in a fair and transparent way when taking action or making decisions on behalf of Visma.

The shared responsibility requires you to be fully familiar with the rules on gifts and hospitality set out in our anti-corruption policy, complete the annual mandatory anti-corruption training, and seek guidance from your leader whenever you are in doubt. In addition, each Visma company must assess the risk of corruption in their businesses.

Visma expects its business partners, including suppliers, distributors, agents and joint venture partners, to abide by the same principles. Read more in the Visma Anti-Corruption Policy.

Always act with transparency. On suspicion of breach of the anti-corruption policy, you are to immediately contact your leader or use Visma's established Whistleblowing Channel.



Conflicts of interest

Conflicts of interest refer to situations where your personal interests, relationships or activities might interfere - or appear to interfere - with your professional responsibilities.
All employees should avoid situations where personal interests might conflict with Visma's interests. Every employee has a personal responsibility to proactively avoid such situations, and act in accordance with good professional judgement.

Remember: As an employee you have a duty to act in good faith and in the best interests of Visma. If you have information about a potential conflict of interest, you are obligated to report it. When in doubt, seek guidance from your leader.

Conflicts of interest most commonly arise in the following situations:

Gifts and hospitality to/from external parties

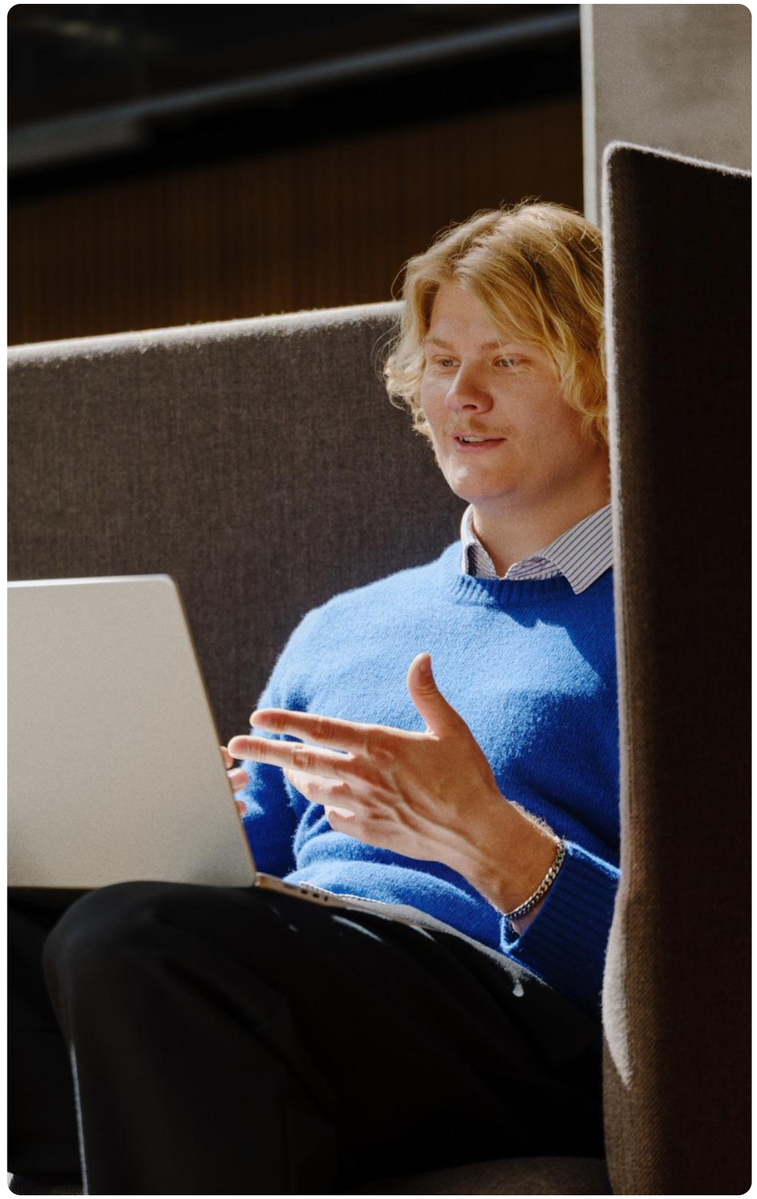
Conflicts of interest can easily occur, or be perceived to occur, when accepting and giving gifts, entertainment or other business courtesies from/to a current or potential customer, supplier or business partner. Always seek guidance from your leader on whether a gift or business courtesy is appropriate and in accordance with our rules on gifts and hospitality. Read more in the Visma Anti-Corruption Policy.

Personal relationships

A conflict of interest arises if a personal relationship could influence professional decisions, such as those related to hiring, promotions, performance management or salary. To ensure fairness and impartiality, it is important to refrain from participating in decision-making processes that involve your relatives, spouse, partner, or other close personal relations.

Political activities

Conflicts of interest may arise if a political purpose is supported, or seems to be supported, by Visma. To maintain Visma's political neutrality, it is important that company resources, including your own work time, company equipment, supplies and inventory are not used for any personal activity or purpose.



Gifts and hospitality

Receiving or giving gifts and hospitality to/from external parties can create actual, potential or perceived conflicts of interest, which could compromise our professional judgment. To uphold Visma's integrity, always be transparent and use prudent judgment in these situations. Any gift or hospitality that could be as an attempt to improperly influence business decisions is unacceptable, particularly during sensitive contractual events like tender processes, contract renewals or contract negotiations. If you are in doubt, seek guidance from your leader.

Gifts

As a general rule, do not accept gifts from, or give gifts to, external parties, except for promotional items of minimal value normally bearing a company logo. Modest gifts within the value limit and within the acceptable categories as stated in the anti-corruption policy are generally acceptable. The limited exceptions, required procedures and gift frequency cap are detailed in the Visma Anti-Corruption Policy.

Hospitality

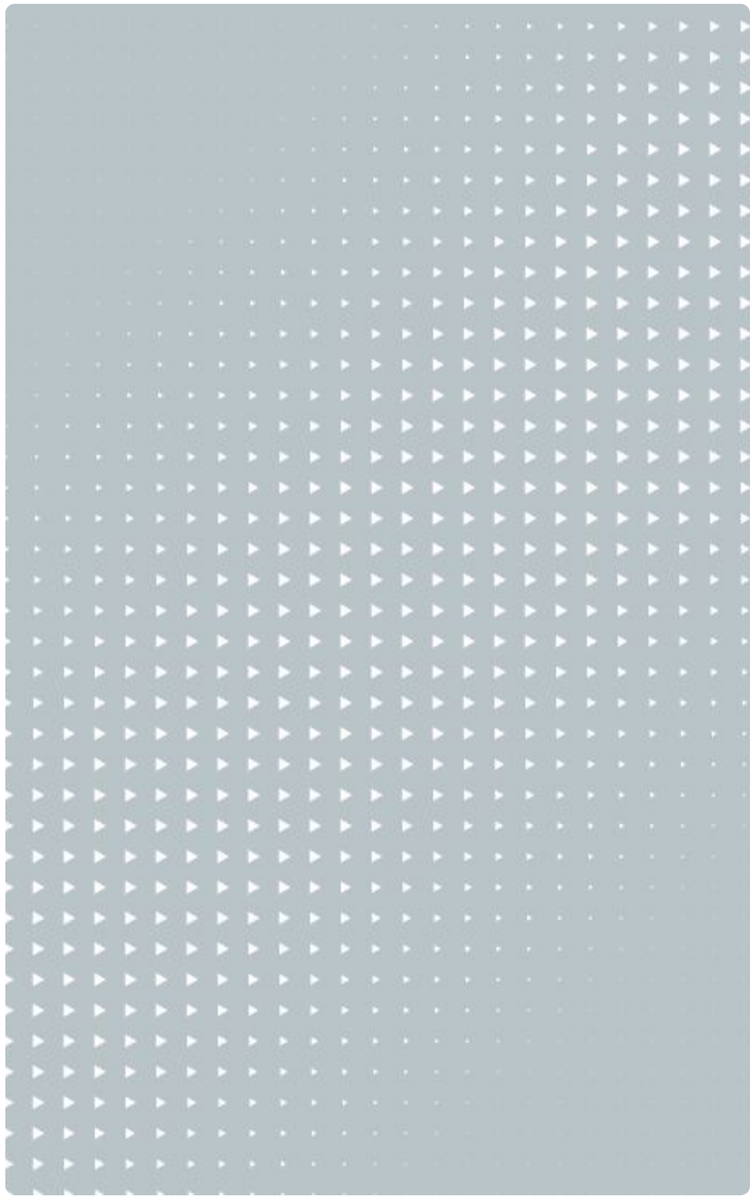
Business hospitality may only be offered or accepted if it serves a clear business purpose and its costs are kept within reasonable limits. Modest hospitality within the value and frequency limits as stated in the anti-corruption policy is generally acceptable. The specific limits, required procedures and prohibited contexts are detailed in the policy.

Anti-fraud

Fraud is defined as any intentional act of deceit, concealment, or violation of trust to obtain an unfair or illegal advantage (financial or otherwise) for yourself, Visma or another party. It includes all forms of intentional misappropriation and misrepresentation, such as theft, embezzlement, falsification of records, misrepresentation of information, and any other dishonest fraudulent act performed individually or in collaboration with others.

Visma has zero tolerance for fraud and is committed to acting professionally, fairly, and with integrity in all business activities and relationships. Any fraudulent activity performed will not be tolerated and will be subject to disciplinary action.

If you suspect or become aware of any indication of fraud, you shall immediately report to your leader, or anonymously through the
Whistleblower channel. All concerns can be raised without fear of retaliation.



Accurate records

All records, and accounts should give a true and fair representation of the financial position of the company or Visma group. Every business transaction shall be properly authorised and recorded in a timely manner.
No employee may ever make a false or misleading entry in any company or Visma group record. This includes everything from individual expense reports and timesheets to major financial statements. Falsifying records not only violates company policy, leading to disciplinary action up to termination, but can also expose you and the company to civil and criminal penalties.

Anti-money laundering

Global laws are in place to combat money laundering and financing of terrorism.

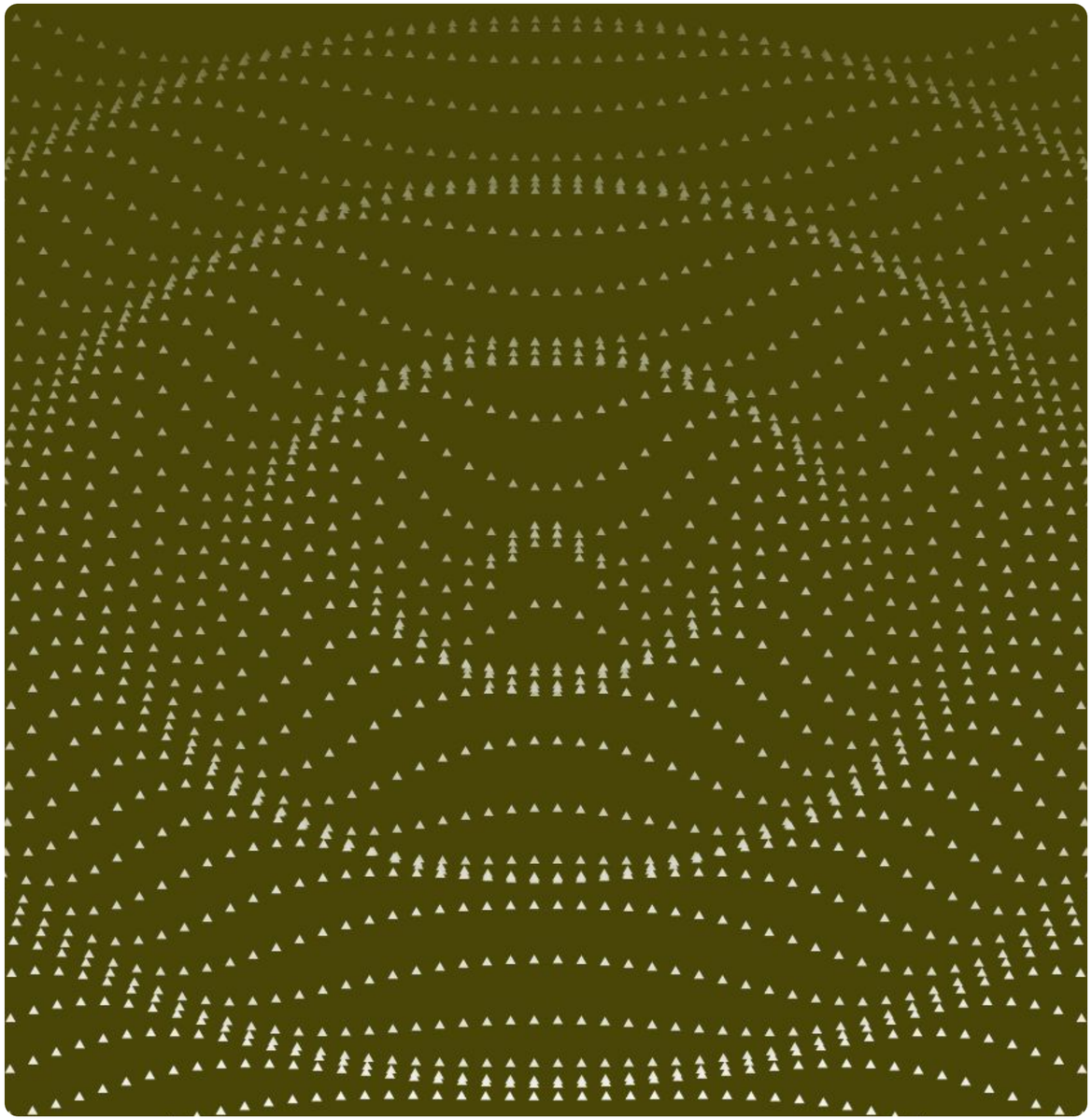
- Money laundering occurs when funds or other assets originating directly or indirectly from criminal offenses are put into circulation in the economy, eventually making their source appear legal.
- Financing of terrorism occurs when money or other resources are made available to commit criminal acts of terrorism or to support terrorist organisations.

Visma assets - including software, tools, equipment, and services - must not be used or made available, directly or indirectly, for money laundering or financing terrorism.

At Visma, we actively combat money laundering and terrorism financing through assessing the risks, customer due diligence, and ongoing monitoring of relationships and transactions. We identify and address red flags or suspicious transactions with appropriate follow-up. We strictly avoid involvement in illicit financial flows and comply with all relevant laws and regulations.

Example: If a customer overpays and requests the excess be refunded to an alternative account (e.g., in a different country) or in cash, do not accept the request immediately. Ask for an explanation as to why the refund cannot be processed via the original payment channel.

Consult your local AML/CFT officer or the Group support.



Competition and market regulations

As an employee, you have a responsibility to understand and adhere to national, EU, UK law (due to Brexit) and international competition law and policies in order to minimise risk for Visma.

Visma is committed to competition that is fair and in accordance with all national, EU, UK and international law. Such regulations seek to prevent corporations from weakening competition, thereby harming consumers and society through higher prices, less choice, poorer product quality and reduced innovation. Examples may be:

Cooperation between two or more companies to restrict competition on pricing, divide markets between them, or limit technological innovation and development.

A single company using a dominant position in a broad or narrow market to impose unreasonable prices or limit production to hurt other companies in that market.

On suspicion of breach of anti-competitive law or policy, you are to immediately contact your leader, or use Visma's established Whistleblowing Channel.

Each employee and leader should:

- Never take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, blackmail, misrepresentation of material facts, or other illegal trade practice.
- Never engage in price fixing, bid rigging (collusion in which bidders on a contract decide who should be successful in the tender, and then draft their bids accordingly), allocation of markets or customers, or similar illegal anticompetitive activities.
- Understand that the purpose of minor and limited business entertainment (restaurant visits or events) and gifts in a commercial setting is purely to create goodwill and sound working relationships. It is not to gain unfair advantage with customers, vendors or government representatives.
- Never accept a gift from an external party, in person or by a family member in a Visma setting, unless the gift (1) is not a cash gift and is in accordance with Visma's anti-corruption policy, (2) is consistent with customary business practices, (3) is of reasonable low value, (4) cannot be construed as a bribe or payoff, (5) does not violate any laws, regulations or applicable policies of the other party's organisation, and 6) has been declared to your leader or with objective certainty is appropriate.



Sanctions and export control

In recent years, sanctions and export control have become important tools for individual countries, the EU, and the United Nations. These measures aim to reduce the influence and funding of targeted regimes and to pressure entities towards resolution and prevention of armed conflict. At Visma, we must always comply with national, EU and UN sanctions and export control legislations, as well as internal policies and keep track of new developments in the field.

Cross-border business processes and transactions may be subject to prohibitions, restrictions, approval requirements, or other supervisory measures under export controls and sanctions. These may apply to:

- customer and business partners,
- goods and services (including technologies, software and technical cross-border transfers and transmissions (e.g. by e-mail or cloud),
- countries and regions,
- financial resources,
- end-use of the products, services and resources.

Should you become aware of export control and sanction legislation being violated in your area of responsibility, immediately inform your local legal counsel, local management and Visma Group Legal Counsel and contribute to remedy such violations and to prevent them from occurring again in the future.

Example: If a potential customer (as a legal entity or through an executive management member) is on a sanction list, or if the customer is registered or operates in a sanctioned country, you must discuss the situation internally and escalate it appropriately. This coordination is crucial to ensure compliance with relevant legislation and to manage inherent risks effectively.

Responsible use of AI

We expect and encourage every employee to use AI tools to work better by moving faster, thinking sharper, and spending less time on the repetitive tasks, so you can do more of what matters. See the Visma AI Code of Conduct presentation and full version for details and tips.

The following principles guide the application of AI in our daily work:

01

Fairness and Inclusivity

Visma's AI systems must be designed to be fair and inclusive, with all individuals treated justly. It's our responsibility to actively identify and mitigate harmful bias in any AI models and data that are used or created.

02

Transparency and Reliability

We are committed to understanding how our AI systems make decisions. When using or developing AI, the technology must be reliable, and there must be clear accountability for its outcomes.

03

Security and Privacy by Design

Upholding the highest standards of privacy and security is crucial. It's our responsibility to follow our policies and guidelines on data protection and security.
This includes avoiding unapproved AI tools ('Shadow AI'). See the Visma Information Security Policy for the full security requirements.

04

Environmentally Sustainable Use

We are aware of the energy and water consumed by AI systems. Therefore, we are responsible for their efficient and sustainable use, which can be achieved by following the core principles outlined in Visma's Environmentally Sustainable Use of AI Tools guideline.

All use of Artificial Intelligence should adhere to the Responsible AI guidelines at Visma.

03

Safeguarding assets

In Visma, we act responsibly with Visma's assets and use them only for their intended purpose. Assets includes hardware, intellectual property, information and data.

- Companies' assets
- Confidential information
- Data protection
- Cost control and tax practices
- Representing Visma in public

Companies' assets

Why protecting company assets is crucial

Visma's success and competitive edge are built on a foundation of assets. These assets - including innovative software, strategic business plans, and customer data - are the result of significant investment and hard work. Protecting them is not just a company policy; it's essential for maintaining our position as a market leader, ensuring business continuity, and safeguarding our employees' future. When we protect these assets, we're protecting our collective interests and shared success.

Visma spends considerable resources to develop and maintain our assets. All Visma employees should follow applicable security guidance and use procedures to protect Visma assets from theft, loss, damage and misuse, including unauthorised access. The detailed requirements for asset management, access control, and incident reporting are set out in the Visma Information Security Policy.

Protecting intellectual property

Good ideas, inventions and business strategies are what makes Visma one of the leading companies in its field. Visma's assets and confidential information about our businesses represent many years of hard work and deserve protection. As an employee, you are entrusted to protect these assets and information, and by that protect Visma's competitive advantage.

Protecting Visma's physical property

In addition to protecting Visma's intellectual property, it is important to maintain sufficient security routines to protect Visma's equipment and facilities. Carefully consider the Visma Physical Access Policy.

All resources, including physical, building, hardware, equipment etc., and non-physical resources, such as data processed, should only be used to enhance Visma's businesses. It is every employee's responsibility to protect our assets and resources from abuse and waste.

Your Visma mobile device, computer or removable storage with Visma- or customer-owned information must never be left unattended in public spaces. Devices must be used according to the Visma Personal Computer Management Policy.

Confidential information

How do I protect confidential information?

At Visma we expect and encourage knowledge sharing and transparency. We have a duty to share information over hiding information. These principles makes Visma resilient and stimulates innovation.

In this transparent and sharing culture we acknowledge that parts of the information that we store, process and transport requires protection from those that can do Visma or our Customers harm. Such protective measures help Visma and our Customers maintain our competitive advantage as well as build and maintain trust from our customers, partners and society at large. Information that require protection come in many forms, from written documents and records, electronic data to oral communications.

Always have in mind that our customers trust us with their data. It is our duty to protect their interests and all Visma employees are bound by the confidentiality clauses in our employment contracts. They are there to protect our customers, your colleagues as well as your own personal information.

Information that require protection must be marked in a way that makes it apparent that there are conditions for the treatment, storage and usage of the information that applies. To help identify and classify information that needs protection vs information that can be freely shared, Visma has devised policies and guidelines.

The Visma Information Classification and Handling Policy provides guidelines and detailed advice for all Visma colleagues. For the broader security framework refer to the Visma Information Security Policy.
Use this guideline if authorities request access to customers' data.

The basic principle is that the author of information should clearly mark it with what type of classification it has, whether restricted access is needed, and how to store, transmit and process it in a safe way.

Examples of information that require protection:

- Security information that may give an attacker an advantage (e.g. your password)
- Detailed sales information that may give competitors an advantage (e.g. our price breakdown structure in bids, information about new products that are not public, business strategies, contract details that are important for our business conduct)
- Personal and sensitive information (e.g. payroll, medical data)
- If employees are bound by the confidentiality clauses in the employment contract. This responsibility also continues even if the employee leaves Visma.

Best practices



Marking

Every document, file or discussion thread containing sensitive data should be clearly marked with its classification (e.g., Visma Internal, Visma Restricted). This is the first and most important step. It's like putting a label on a container so everyone knows what's inside and
how to handle it.



Access Control

Access to sensitive information should be limited to those who genuinely need it to do their job. This principle of least privilege minimizes the risk of unauthorized access and data breaches.



Secure Handling

Whether you're sending an email, storing a file, or having a discussion, always use secure methods. This means using the provided secure channels, secure storage, as well as being mindful of your surroundings when discussing sensitive topics.



Using Third-Party Software Applications

Before downloading or using any third party software application that lacks an existing contract and a data processing agreement (DPA) with the Visma Group (or your local Visma company), you must thoroughly review its specific Terms & Conditions and be aware of the specific permissions you grant to the third party application. This rule applies to all online third party software applications, including those available in Google Marketplace, Chrome Extensions, Slack, etc. You should strictly avoid entering any confidential or business-sensitive information into these third party applications, and you must never enter personal data or customer data.

This includes AI-powered tools: avoid using any AI service that has not been approved by your local IT or Security team ("Shadow AI"), in line with the Visma Information Security Policy.

Data protection

At Visma, keeping personal data safe is a key part of our work. Here's what you need to know initially:

Handling personal data
All employees shall handle personal data in accordance with the Visma Privacy Policy.

Data Protection Training
Everyone at Visma must finish all required training on data protection. This training covers the basics of GDPR, important rules for handling personal and customer data, and how to apply these rules in our daily tasks. You will receive separate information about this.

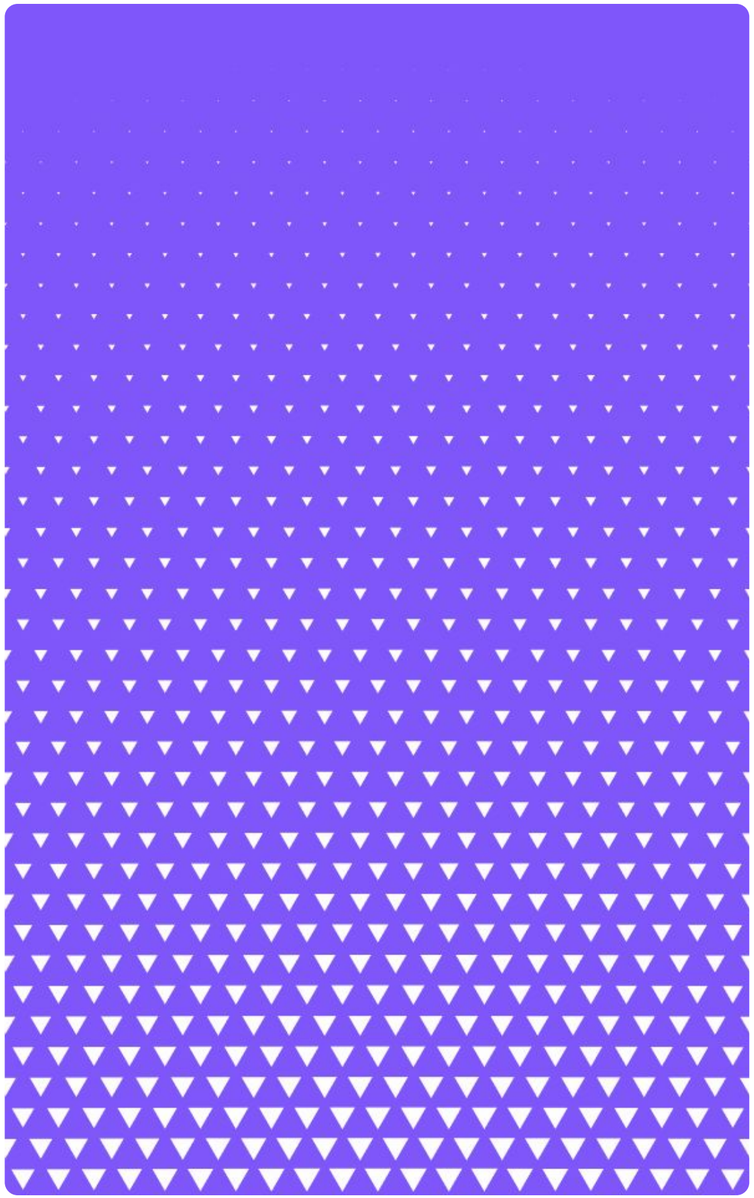
Customer data
We must always protect customer data according to our agreements with them. Make sure that your handling of personal data on the customer's behalf is in accordance with the customer contract.

Visma's data
When using personal data for your own company's needs, make sure to follow your company's privacy statement and internal policies.

Security and privacy by default Services and solutions that we provide to our customers or colleagues must be delivered as secure and private by default.

Reporting
If you discover a problem with personal data security - for example, that personal data has been lost, disclosed to someone that should not see the data, or unintentionally interfered with - report it immediately at security@visma.com. Also, any questions or requests about personal data, whether from inside or outside the company, should go to your company's Data Protection Manager.

Questions?
If you have questions about how to handle personal data, look at the Visma Privacy Policy or talk to the Data Protection Manager for your company. They're here to help make sure we do things right.





Cost control and tax practices

Cost control
All employees are responsible for Visma's finances - not only the people in finance. This means that when entering into contracts on Visma's behalf, e.g. paying for a service, you should always think about how Visma's assets are spent, if the action is necessary, and whether it is good for Visma's business.

You are an important part of Visma's financing, whatever your role is in the company

Remember to:

- Enter into agreements in accordance with your level of authority, Visma's best interest, and relevant policies.
- Use Visma's equipment with care and in a sustainable manner.
- When travelling on behalf of Visma, use public transport to the extent possible and always consider using technologies such as video conferencing for meetings.
- When travelling on behalf of Visma, use common sense and follow company and Visma group policies. When booking hotels and buying meals, find affordable options.

Tax practices:

We will not engage in or facilitate any activity that constitutes any illegal evasion of taxes and each employee should contribute to this commitment.

Representing Visma in public

Social media
Social media should be used to reach out to our customers, build trust, and give them the opportunity to provide us with feedback. When acting on behalf of Visma on social media, it is important to always portray Visma in the best interest of our company. When you use social media on behalf of Visma, our Social media strategy shall always be followed.

How should we act on social media?
Be honest and truthful, and stick to the facts. Always be polite, respectful and professional. Never speak badly about others, customers, employees, competitors, etc.
Let your leader know if you detect negative comments about Visma on social media.
Do not post confidential or financial information. If unsure, seek guidance before posting anything on social media.
Never comment on potentially damaging incidents or negative publicity on social media.

Public appearances and press
Public appearances on behalf of Visma shape the perception of Visma as a company. It is important to remember to represent Visma in the best possible way. This means that you should always be well prepared, professional and polite.
Before you represent Visma in public, e.g. participating in a panel discussion or giving
a presentation at a public event, you need permission from your leader.
It is important that Visma is unified regarding any information that is released publicly about our company. To ensure there is an overview of what information is given and to whom, Visma employees should never talk to the press unless it is approved by either your Managing Director, the person responsible for PR on a country level, or Visma group PR.
Enquiries from financial analysts or investors should be passed on to the Investor Relations department.

Key principles for representing Visma in public:

- Be well prepared.
- Ensure that any professional presentation reflects our values.
- Always answer questions in a polite and professional manner.
- Never share non-public or confidential information about Visma, our customers, partners, or internal processes. This includes financial information/projections, organisational changes or unreleased products. Avoid commenting on rumours or speculation.
- If a crisis should occur, communication should always be made in accordance with the Crisis Management Plan.

04

Speak up and make a difference

For Visma, your voice is an important part of our commitment to safety, integrity and transparency. If you experience something wrong, say something - whether it's a concern or a potential or actual breach of the law, our internal guidelines and policies or our values.
We prioritize your confidentiality and ensure your insights are valued and protected. Join us in fostering a safe, ethical workplace where everyone can thrive.

Visma will not tolerate any form of misconduct or critical conditions, such as violations of statutory rules, internal rules, policies or ethical standards, such as bullying, harassment, discrimination, corruption, money laundering or any other financial fraud, and will make efforts to ensure a safe and healthy environment in all our business activities and companies.

Visma will comply with all applicable laws and regulations and act ethically and socially responsible. Breaches of any local and/or EU/EEA law may result in disciplinary actions, including termination / dismissal and reports to the relevant authorities.

The Visma Whistleblowing Channel is a tool enabling anonymous reporting of any suspected breach of the local and/or EU/EEA law from both inside Visma and outside. To understand how to report a (potential) breach of the law or our values, please read the full procedure here.

Code of Conduct

June 2026

Visma AS
Group Legal and Compliance team

Main office:
Karenslyst allé 56, 0277 Oslo, Norway

Postal address:
PO box 733, Skøyen 0214 Oslo, Norway

Telephone: +47 46 40 40 00 (08:00–16:00 CET)

visma@visma.com
Visma on LinkedIn