CODE OF CONDUCT

Date of Issuance: 20 September 2016
Date of Most Recent Update: 16 May 2023

1 TABLE OF CONTENTS

1 Table of contents 2
2 Introduction and Scope 3
2.1 Scope 3
2.2 Gimv Compliance & ESG Office 3
2.3 Violations of the Code of Conduct 4
2.4 Consultation, acknowledgement & actualizations 4
2.5 Definitions 4
3 Interactions with portfolio companies 5
3.1 Listed portfolio companies 5
3.2 Non-listed portfolio companies 5
3.3 Compensations for assignments in portfolio companies 5
4 Business ethics and integrity 6
4.1 Responsible investments 6
4.2 Work environment 7
4.3 Confidential information 7
4.4 Conflicts of interests 7
4.5 Use of Gimv resources 8
4.6 Fair competition 8
4.7 Gifts and bribery 8
5 External communication & Social media 8
6 Rules & Regulations 9
Annex 1 Form of acknowledgement 10
Annex 2 Gimv Whistleblowing Policy 11
Annex 3 Gimv Data Protection Framework 12
Annex 4 Gimv Expense policy 13
Annex 5 Gimv IT User Policy 14

2 INTRODUCTION AND SCOPE

2.1 SCOPE

This ***Code of Conduct*** as approved by the Board of Directors of Gimv is applicable to every employee (including temporary employees and interns) of Gimv and its subsidiaries (an "***Employee***") as well as every member of the board of directors of Gimv (a "***Director***") (an Employee and a Director are hereafter jointly referred to as an "***Addressee***"). For the avoidance of any doubt, subsidiaries do not include in any way the external portfolio companies of Gimv nor the Gimv-Belfius infrastructure joint venture TDP, TINC and TDP-managed funds.

This Code of Conduct provides important general guidance. It is however not an exhaustive document anticipating every situation an Employee or a Director may face in their day-to-day activities. Gimv expects that the Addressees always act in a responsible and diligent way. In case an Addressee has questions or is uncertain about the provisions of the Code of Conduct or whether a certain act would go against the provisions or the spirit of the Code of Conduct, Gimv advises such Addressee to immediately contact the Gimv Compliance & ESG Office.

The Code of Conduct relates to (i) interactions with portfolio companies (both dealing in portfolio company securities and receiving compensations for assignments in portfolio companies), (ii) setting the standard as an Employee or Director of Gimv on the areas of respect and integrity, and (iii) communication to the public. Certain principles of the Code of Conduct are further elaborated by specific policies or procedures. As such, the Gimv Whistleblowing Policy, the Gimv Data Protection Framework, the Gimv Expense Policy and the Gimv IT-policy are added as annexes to the Code of Conduct and are considered as an integral part thereof. For the applicable internal rules on Dealings in Gimv Securities, we refer to the separate Gimv Dealing Code.

The Code of Conduct reflects certain fundamental principles which Gimv values highly and policies or procedures to which the Addressees must comply. The Code of Conduct does however not create any right for any government, shareholder, Portfolio Company, supplier, competitor or any other person or entity.

The Code of Conduct and its annexes may be subject to updates and modifications based on new laws and regulations or new significant developments in society. All Addressees will be informed by email of any changes to this Code of Conduct. The latest version of the Code of Conduct can at all times be consulted on the Gimv Intranet or Gimv website.

2.2 GIMV COMPLIANCE & ESG OFFICE

The Gimv Compliance & ESG Office, which today consists of the persons listed below, has been appointed by the Board of Directors of Gimv to supervise compliance with this Code of Conduct and to deal with the matters specified herein.

- Koen Dejonckheere, Chief Executive Officer
- Edmond Bastijns, Chief Legal Officer – Secretary General
- Kristof Vande Capelle, Chief Financial Officer
- Vincent Van Bueren, Compliance & ESG Manager .

If you have any questions or are in any doubt on how to comply with this Code of Conduct, please contact the Gimv Compliance & ESG Office by email on compliance@gimv.com.

2.3 VIOLATIONS OF THE CODE OF CONDUCT

Any violation of the Code of Conduct and its annexes will not be tolerated. Such violations can lead to disciplinary actions consistent with applicable laws (including but not limited to labor, criminal and corporate laws) and regulations.

In case an Addressee has a compliance concern (i.e. has any knowledge of any behavior, which is or might be inconsistent with or go against the Code of Conduct and its annexes and will or might impact the integrity of Gimv as an organization), Gimv encourages such Addressee to speak up. He/she can report it to the Gimv Compliance & ESG Office (compliance@gimv.com), in line with the Gimv Whistleblowing Policy (attached as Annex 2).

Gimv does not tolerate (i) any form of (direct or indirect) retaliation against an Addressee who in good faith seeks advice, raises a concern or reports misconduct, nor (ii) any abuse of the Gimv speak up channels. Disciplinary actions may be taken in such cases.

2.4 CONSULTATION, ACKNOWLEDGEMENT & ACTUALIZATIONS

The Code of Conduct is permanently available for Employees on the Gimv Intranet and for Directors on the Gimv website. Each Employee receives a copy of the Code of Conduct upon its issuance and Employees who start their employment following the Date of Issuance receive a copy thereof on or shortly after the date on which they start their employment at Gimv. Directors receive a copy of the Code of Conduct on or shortly after the date of their appointment.

All Addressees acknowledge being aware of, being bound by and undertake to comply with the Code of Conduct and its annexes, for which they will sign a declaration in the form attached as Annex 1.

2.5 DEFINITIONS

The following definitions apply, unless the context requires otherwise:

Addressee has the meaning given to it in section 2.1.

Closely Associated Person or ***CAP*** means, in relation to an Addressee:

i. a spouse, or a partner that is legally considered to be equivalent to a spouse;
ii. a child for which the Addressee legally bears responsibility (which includes adopted children);
iii. a relative who has shared the same household as the Addressee for at least one year on the date of the relevant Dealing; or
iv. a legal person, trust or partnership, the managerial responsibilities of which are discharged by the Addressee or by a person referred to in point (i), (ii) or (iii), which is directly or indirectly controlled by the Addressee or such a person, which is set up for the benefit of the Addressee or such a person, or the economic interests of which are substantially equivalent to those of the Addressee or such a person.

Code of Conduct has the meaning given to it in section 2.1.

Date of Issuance means the date on which the current Code of Conduct has been formally approved by the Board of Directors of Gimv for the first time and from when it became applicable to all Addressees.

Date of Most Recent Update means the most recent date on which the Code of Conduct has been amended upon approval of the Board of Directors of Gimv.

Dealing should be interpreted as including any transaction, in the broadest sense, in respect of Securities.

Director has the meaning given to it in section 2.1.

Employee has the meaning given to it in section 2.1.

Gimv Compliance & ESG Office has the meaning given to it in section 2.1.

Gimv Non Trading List means the overview of listed Portfolio Companies of which the Securities may not be traded by the Addressees and their CAPs. This overview is kept and maintained by the Gimv Compliance & ESG Office and available for all Addressees on the Gimv Intranet.

Portfolio Company means any entity in which Gimv-group holds an investment (by means of Securities or otherwise) as part of its daily business activity.

Securities means any shares and debt instruments and any derivatives and other financial instruments in the broadest sense linked thereto.

3 INTERACTIONS WITH PORTFOLIO COMPANIES

3.1 LISTED PORTFOLIO COMPANIES

Employees, Directors and their Closely Associated Persons (CAPs) are only allowed to make Dealings in Securities issued by listed Portfolio Companies in case such Dealings are allowed under the dealing code of such listed Portfolio Company and provided that such listed Portfolio Company is not mentioned on the Gimv Non-Trading List. The Board of Directors can allow in exceptional circumstances a Dealing in Securities issued by listed Portfolio Companies which are mentioned on the Gimv Non-Trading List (for example in case of an inheritance).

3.2 NON-LISTED PORTFOLIO COMPANIES

It is explicitly prohibited that an Employee or a Director holds, directly or indirectly, Securities in non-listed portfolio companies. Employees and Directors will take the necessary required and reasonable precautions to prevent that such interests are being held by their respective CAPs. This general prohibition stands with the exception of any explicit and written exemption that may be authorized by the Board of Directors and subject to the conditions of such authorisation.

3.3 COMPENSATIONS FOR ASSIGNMENTS IN PORTFOLIO COMPANIES

For the avoidance of any doubt, this section 3.3 does not apply to any Director who would hold a position as member or observer of a board of directors, a supervisory board or an advisory board (non-exhaustive list of positions and corporate bodies) of a listed Portfolio Company of Gimv.

All compensation, of whatever kind, that Employees are entitled to by virtue of a position as member or observer of a board of directors, a supervisory board or an advisory board (non-exhaustive list of positions and corporate bodies) of a Portfolio Company of Gimv, should be paid to Gimv (or the entity of Gimv-group designated thereto), in preference directly by such Portfolio Company to Gimv. In case such compensation has been paid to an Employee, the Employee will transfer such compensation immediately to one of the bank accounts of Gimv as mentioned on the Gimv stationery.

Compensation as meant in this article includes (non-exhaustive) fixed or variable directors' remuneration, attendance fees, emoluments, management fees, services or consulting fees and all other similar forms of compensation.

4 BUSINESS ETHICS AND INTEGRITY

The ambition of Gimv is to build and grow outperforming companies in attractive growth markets by creating value in terms of strategy and business modelling, international expansion and operational excellence. In this context, Gimv has translated its vision of the sustainable future of the economy and society into five investment platforms: Consumer, Healthcare, Life Sciences, Smart Industries and Sustainable Cities.

In realizing its ambition, Gimv expects high ethical standards, a continuous exemplary behavior and a striving to excellence from its Portfolio Companies and their directors, executives, managers, employees and other representatives. Therefore, Gimv and their Employees and Directors are obligated to set the standard on the areas of respect, business ethics and integrity.

Moreover, Gimv is committed to only work with third parties (including intermediaries and advisors) whose conduct is consistent with the standards and principles set out below.

4.1 RESPONSIBLE INVESTMENTS

Gimv is a leading, responsible and society-conscientious European private equity firm. Therefore, Gimv commits not to invest itself and to watch over that its Portfolio Companies will not invest in following companies or businesses:

- of which the activities, products or services are deemed illegal under any applicable law, regulation or global convention in the relevant jurisdiction (including but not limited to slavery, exploitation, forced labor, human trafficking, child labor, prostitution, illegal substances or any form of organized crime);
- which are involved in the production, sale, use of or trade in arms, weapons of mass destruction or inhuman weapons or critical components associated thereto (including but not limited to nuclear, chemical, and radiological weapons, landmines and bombs). Goods, services or smart technologies and solutions which are defensive or non-offensive within areas such as avionics, radar, sonar, instrumentation, communication and protection (non-exhaustive) can be in line with the responsible investment policy of Gimv after proper assessment by the Gimv Compliance & ESG Office;
- of which the activities directly or indirectly contribute to the financing of terrorism;
- that are active or involved in the development, operation, sale, distribution, management of or trade in products and/or services and/or facilities that are directly or indirectly related to gambling, tobacco or pornography.

When in doubt whether the activities of a (prospect) Portfolio Company may fall within the abovementioned criteria, please contact the Gimv Compliance & ESG Office.

Gimv expects from its Portfolio Companies that they are a committed, constructive and trustworthy partner who commit to:

- comply with applicable laws, regulations or global conventions;
- respect competition law in its dealings with competitors, suppliers and customers;
- never participate in any bribery, corruption or similar behavior;
- uphold high standards of business integrity and behave in proper ethical way, including but not limited to:
    - having a responsible and sustainable approach of the environmental management of its business;
    - respecting the rights of its employees, treating them fairly and safeguarding a healthy and safe work environment;

- installing a proper governance, risk management and compliance culture.

4.2 WORK ENVIRONMENT

All Addressees should respect the distinctions of the individuality of every person active within Gimv as an Employee or as a Director. All Addressees should therefore respect one another and realize Gimv's objectives together without regard to race, ethnicity, religion, national origin, gender, sexual orientation, disability, age, family status or any other basis. Any form of unlawful discrimination or improper/unacceptable (sexual) behavior will not be tolerated.

Gimv values highly having and maintaining a work environment in which people are treated with dignity and respect and that is characterized by mutual trust and the absence of any (direct or indirect) form of intimidation, oppression and exploitation.

4.3 CONFIDENTIAL INFORMATION

All Addressees have or may have access to confidential information with respect to (i) Gimv, (ii) the business activity of Gimv as a private equity company conducting investments in Portfolio Companies, and (iii) (potential) Portfolio Companies of Gimv and third parties. All Addressees must therefore take the necessary precautions to guard the confidential character of such information and prevent any unlawful disclosure to competitors or other unauthorized third parties. To protect the integrity and security of its own data, Gimv has put in place the Gimv Data Protection Framework designed to detect and alert unlawful data breaches or losses from inside the organization. A detailed description of how the Gimv Data Protection Framework works (including how Gimv handles any possible impact on the privacy of the Employees) is added to the Code of Conduct as Annex 3.

4.4 CONFLICTS OF INTERESTS

Conflicts of interests may arise when having a direct or indirect personal interest in a decision taken by and for Gimv. In case of a conflict of interests, the impartiality of any decision is not guaranteed.

Therefore, in addition to the rules of the Belgian Company Code applicable on conflicts of interests of Directors or members of management committees, all Addressees shall exercise fair, objective and impartial judgment in all business dealings of Gimv, thereby always placing Gimv's interest over any personal interest relating to matters of business of Gimv.

All Addressees will not use their position to obtain any direct or indirect personal benefit and will disclose to the Gimv Compliance & ESG Office any conflict of interests, any relationship they have with a (potential) Portfolio Company other than the relationship arisen in the daily business context of Gimv, a third-party supplier or consultant working for Gimv or a competitor of Gimv. The Gimv Compliance & ESG Office reserves the right to inform the Board of Directors of Gimv of such disclosed conflict of interests. All Addressees must refrain from being involved in any transaction or business activity that could be considered to be or may give rise to a conflict of interest.

In case an Addressee is not sure if a certain situation represents a conflict of interests or not, he/she is encouraged to seek guidance from the Gimv Compliance & ESG Office.

4.5 USE OF GIMV RESOURCES

The Addressees are not allowed to use any resources, assets or solvency of Gimv (or any other entity of Gimv-group) or a Portfolio Company for gains outside the ordinary course of business of Gimv or illegal purposes. Gimv understands that Employees from time-to-time may need to address personal matters during worktime that cannot be handled outside of normal work hours, whereby such use of worktime may not be excessive. In case of doubt, the Employee is encouraged to seek approval from the relevant department head.

For the guidelines about the correct use of the Gimv IT facilities and environment, we refer to a separate IT policy, which is added to this Code of Conduct as Annex 5 and can also be consulted on the Gimv Intranet.

4.6 FAIR COMPETITION

Gimv highly values fair competition and wishes to conduct its business activity in an ethical way and with integrity. Therefore, Gimv does not and will never make investments or enter into business arrangements that distort, eliminate or discourage competition or that provide improper competitive advantages.

4.7 GIFTS AND BRIBERY

Gimv is a commercially active company and as such acts with its Portfolio Companies, consultants, service providers and all other parties in accordance with reasonable and common commercial practices. As a consequence, the offering or acceptance by Addressees of everyday gifts and favours as well as occasional meals are considered as being in accordance with reasonable and common commercial practices when they are modest (in value and frequency) and appropriate (both time and place). Under no circumstance the exchange of cash or cash equivalents is acceptable.

Gimv in any way formally prohibits bribes and gifts to be distributed, offered or accepted that should serve to obtain or retain business or other improper advantages or promises. Finally, the disguising of gifts or entertainment as charitable donations is considered as a violation of the Code of Conduct.

In case an Addressee is not sure whether a certain situation falls within the reasonable and common commercial practices or not, he/she is encouraged to seek guidance from the Gimv Compliance & ESG Office.

Gimv may take action (including legal proceedings) at any time against Employees, Directors, (potential) portfolio companies, consultants or service providers (non-exhaustive) that make themselves guilty or are guilty of (participating in) bribery, fraud, price fixing, invoicing services that they did not provide, corruption or attempted corruption.

5 EXTERNAL COMMUNICATION & SOCIAL MEDIA

The Chairperson, the CEO, the other members of the Executive Committee and any other person specifically designated thereto are the only persons responsible for the external communication of Gimv and for maintaining contacts with the media. As such, all questions from the media (in whatever form) must be passed on immediately to one or all of these aforementioned persons.

All Addressees must contribute to protecting and improving the image of Gimv. Consequently, all Addressees must be aware of what they write about Gimv on websites, blogs or social media including but not limited to Facebook, Twitter and LinkedIn. Gimv has made some internal Social Media Guidelines available to the Addressees on the Gimv Intranet.

6 RULES & REGULATIONS

Conducting business in accordance with the highest ethical standards evidently brings along respect for the rule of law and compliance with prevailing legislation. Any breach of law or regulations may result in sanctions of a civil, administrative or criminal nature imposed on Gimv and the individual Addressee involved. This may bring along negative consequences for the career of the individual Addressee involved. In case of any question concerning prevailing legislation, please consult the Gimv Legal Department or the Gimv Compliance & ESG Office.

ANNEX 1
FORM OF ACKNOWLEDGEMENT

To: Gimv NV

Karel Oomsstraat 37

2018 Antwerp

Belgium

(hereafter the ***Company***)

I hereby acknowledge receipt of the Code of Conduct of Gimv including its annexes (i.e. the Gimv Whistleblowing Policy, the Gimv Data Protection Framework, the Gimv Expense Policy and the Gimv IT-policy) provided to me with this acknowledgement.

I confirm that I have read, understood and agree to comply with the Code of Conduct and its annexes, as amended from time to time.

Signature:……..

Date:……

Please complete and return this form to the Gimv Compliance & ESG Office by e-mail to compliance@gimv.com.

ANNEX 2
GIMV WHISTLEBLOWING POLICY

WHISTLEBLOWING POLICY

TABLE OF CONTENTS

BACKGROUND **2**

PART 1. REPORTABLE CONCERNS **4**

PART 2. PRINCIPLES **4**

PART 3. WHISTLEBLOWER PROTECTION **5**

1. **Protection *for good faith* reporting** 5
2. **No protection for *bad faith* reporting** 5

PART 4. CONFIDENTIALITY **5**

PART 5. INTERNAL REPORTING **6**

1. **Whistleblowing Manager** 6
2. **Filing of a Whistleblowing Report** 6
3. **Acknowledgment of receipt** 6
4. **Admissibility** 7
5. **Preliminary assessment of the Whistleblowing Report** 7
6. **Internal investigation** 7

PART 6. EXTERNAL REPORTING **7**

1. **Reporting to the competent authority** 7
2. **Public Disclosure** 8

PART 7. TRAINING **8**

PART 8. RECORD KEEPING AND DATA PRIVACY **8**

PART 9. MONITORING AND IMPLEMENTATION OF THE PROCEDURE **9**

1. **Implementation** 9
2. **Monitoring** 9

ANNEX 1: WHISTLEBLOWING REPORTING GUIDELINES FOR STAFF **10**

BACKGROUND

Gimv NV is a limited liability company incorporated under Belgian law with registered office at Karel Oomsstraat 37, 2018 Antwerpen, Belgium and registered with the Belgian Crossroad Bank for Enterprises under number 0220.324.117 (hereafter "**Gimv**" or the "**Company**").

Gimv is committed to the highest standards of openness, integrity, transparency, and accountability. An important aspect of these values is to provide all shareholders, members of management, permanent, temporary, and former members of personnel, agents, subcontractors and other affiliates[1] (hereafter individually addressed as an "**Addressee**" and collectively the "**Addressees**") of Gimv and its subsidiaries (hereafter **"Gimv Group"**) with an effective process to raise concerns about any of the issues listed in this whistleblowing policy and procedure (the "**Whistleblowing Policy"**). For the avoidance of doubt, subsidiaries do not include the external portfolio companies of Gimv Group nor TDP, TINC and TDP-managed funds.

"**Whistleblowing**" is the process whereby an individual raises genuine concerns in good faith about matters which appear to involve serious concerns within Gimv.

Gimv recognises the value of the Addressees reporting concerns about its business and operations (in such an event, the Addressee is qualified as a "**Whistleblower"**).

Gimv therefore encourages Addressees to voice such concerns internally through the filing of a report as appropriate (such a report being a "**Whistleblowing Report"**).

In line with its own commitment, Gimv trusts that all Addressees will perceive speaking up as a positive contribution to protecting and enhancing the work culture, reputation, and success of Gimv. All Adressees have a responsibility to report suspicious activity promptly and in accordance with this Whistleblowing Policy.

The purpose of this Whistleblowing Policy is therefore to provide a framework and process for Addressees to "blow the whistle" internally on internal legal, regulatory, compliance or ethical breaches. It sets out the process by which such concerns can be voiced and be acted upon. It further details when and how protection from reprisal applies, as well as how confidentiality, conflicts of interest and legal privilege (if any) must be managed.

The objectives of this Whistleblowing Policy are to ensure that:

- Addressees have a clear understanding of when and how to speak up and file Whistleblowing Reports;
- Addressees have a clear understanding of the internal functions and steps implemented to secure the independence and effectiveness of the whistleblowing process;
- Gimv is able to act against reported concerns in an effective and timely manner.

[1] This includes all workers in a professional context, actual and former members as well as persons engaged in a recruiting process, i.e. employees, self-employed workers, volunteers, (unpaid) trainees, shareholders, members of management, administrative, or supervisory bodies of Gimv.

PART 1. REPORTABLE CONCERNS

Gimv encourages all Addressees to file a Whistleblowing Report when they have **reasonable and legitimate belief** that any of the following breaches are being, have been, or are likely to be committed in relation to:

- Public procurement;
- Financial services, products and markets, and prevention of money laundering and terrorist financing;
- Product safety and compliance;
- Transport safety;
- Protection of the environment;
- Radiation protection and nuclear safety;
- Food and feed safety, animal health and welfare;
- Public health;
- Consumer protection;
- Protection of privacy and personal data, and security of network and information system;
- Non-compliance with antitrust or competition laws;
- A breach affecting the financial interests of the European Union[2];
- A breach of Gimv's policies and procedures[3];

(such a situation hereafter defined as a "**Reportable Concerns"**).

This Whistleblowing Policy does **not** cover, and a Whistleblowing Report should not be filed, in relation to grievances specific to working conditions, including but not limited to social, labour and employment complaints, which must be dealt in accordance with applicable HR procedures.

Addressees have no responsibility for investigating the matter they (intend to) report. It is the responsibility of Gimv to ensure that an investigation takes place following receipt of the Whistleblowing Report.

PART 2. PRINCIPLES

Addressees must always act in accordance with the following general principles:

- Reportable Concerns must always be reported in good faith, the latter being presumed;
- Reportable Concerns may be reported even without supporting evidence: sufficient belief that a Reportable Concern is taking place or is about to take place is enough;
- Only direct Reportable Concerns should be reported and no "hearsay" statement should be made;
- Reporting concerns may not serve vindictive or personal purposes (which presumably qualifies as bad faith reporting);
- Reportable Concerns may be reported nominatively or anonymously;
- The rights and protections established in this Whistleblowing Policy cannot be waived by any agreement, policy, form, or condition of employment.

[2] Related to the fight against fraud, corruption and any other illegal activity affecting European Union expenditure, the collection of Union revenues and funds or European Union assets.
[3] Gimv's policies and procedures are set out not only to comply with legal and specified obligations but also to reflect appropriate guidance and foster good practice and culture in support of the success of Gimv.

PART 3. WHISTLEBLOWER PROTECTION

1. Protection *for good faith* reporting

Gimv will protect any Addressee who filed a Whistleblowing Report *in good faith*, even if they turn out to be mistaken, from dismissal and any other forms of reprisal, threat or hostile action.

Prohibited retaliatory measures include but are not limited to suspension, lay-off, dismissal or equivalent measures, demotion or withholding promotion, transfer of duties, change of location of work, reduction in wages, withholding of training, discrimination, coercion, intimidation, harassment, … .

Any such form of retaliatory measures may lead to disciplinary measures in accordance with Gimv's applicable rules and policies, up to and including termination of employment, as well as referral to judicial authorities.

This protection is also given to Whistleblowers passing on information they have obtained outside of a professional context.

Such a protection is also granted, where appropriate, to facilitators, colleagues or relatives of the whistleblower who are also in a work-related connection with the Whistleblower's employer or customer or recipient of services, and any legal entity that the whistleblower owns, works for, or is otherwise connected with in a work-related context.

Whistleblowers shall not incur any liability for obtaining or gaining access to reportable information, provided that the obtention of or access to such information does not constitute a separate criminal offence.

2. No protection for *bad faith* reporting

Gimv takes very seriously any filing of a report that is *known to be false* or that is made *in bad faith*, maliciously, recklessly or with a view to personal gain.

If the investigation concludes that an Addressee filed a Whistleblowing Report in bad faith, Gimv may take disciplinary actions against the whistleblower in accordance with its applicable rules and policies, up to and including termination of employment, as well as referral to judicial authorities.

PART 4. CONFIDENTIALITY

Whistleblowing Reports can be filed nominatively or anonymously.

This Whistleblowing Policy guarantees that all Whistleblowing Reports will be dealt with promptly, independently, and thoroughly, without causing any harm to Addressees, their career or reputation. Gimv will protect in all cases the confidentiality and identity of Whistleblowers and other parties involved in the report and the subsequent internal investigation, as appropriate. The person responsible for handling the Whistleblowing Report will act as identity protection manager.

Total discretion is expected from all parties involved in the investigation and any subsequent procedures.

This Whistleblowing Policy also prevents unauthorized personnel from accessing reported information.

The identity of the Whistleblower and other relevant persons may only be waived in any of the following exhaustive events:

- With the express consent of the persons whose identity is protected, knowing that the Whistleblower can identify him/herself at any given time;
- Upon request of competent judicial or regulatory authorities, to the extent that Gimv is legally required to cooperate with these bodies;
- If the Reportable Concern is used in the context of judicial proceedings;
- When seeking advice from an accountant or a lawyer;
- When the information is already in the public domain,

keeping in mind that the primary purpose of this Whistleblowing Policy is to protect good faith Whistleblowers from disciplinary measures, retaliatory actions or damage to reputation or trust.

PART 5. INTERNAL REPORTING

Internal reporting channels should be preferred over external reporting which is subject to specific conditions (see **PART 6.** below).

1. Whistleblowing Manager

Gimv has entrusted the internal responsibility for handling (i.e. receiving and following-up on) Whistleblowing Reports, including for conducting investigations and recommending subsequent actions where appropriate to the Gimv Compliance & ESG Office. Among the members of the Gimv Compliance & ESG Office, the Compliance Manager of Gimv is designated as the "**Whistleblowing Manager"**.

The appointment of a dedicated Whistleblowing Manager guarantees the handling of the matter in accordance with the governance principles of competences, diligence, fairness and impartiality.

2. Filing of a Whistleblowing Report

Whistleblowing Reports must be filed with the Whistleblowing Manager, by email, in compliance with the guidelines provided to Whistleblowers in **ANNEX 1**.

By exception, where it is not appropriate for the Whistleblowing Manager to conduct the investigation (e.g. because of conflict of interest, including when the Whistleblowing Manager is the subject of the report), the Whistleblowing Report can be filed with one of the other members of the Gimv Compliance & ESG Office, including the CEO, CFO and CLO – Secretary General or the Chairman of the board of directors of Gimv.

3. Acknowledgment of receipt

The Whistleblowing Manager must acknowledge receipt of the report to the Whistleblower within seven (7) working days of its filing (unless the report was filed anonymously).

The Whistleblowing Manager indicates at this occasion, where appropriate and to the extent possible, whether the Whistleblowing Report falls within the scope of the Whistleblowing Policy and is therefore considered to be admissible, including the rights and obligations attached to such reporting and the subsequent steps to be taken. It also clarifies that a meeting may be arranged upon request of the Whistleblower.

4. Admissibility

Upon receipt of a whistleblowing report, the Whistleblowing Manager ascertains the admissibility of the report, which is subject to the following cumulative conditions:

- The facts reported fall within the scope of the Whistleblowing Policy, i.e. consist in a Reportable Concern;
- The reporting persons falls within the scope of the Whistleblowing Policy, i.e. qualifies as a Whistleblower; and
- The formal requirements for a Whistleblowing Report have been met.

5. Preliminary assessment of the Whistleblowing Report

Where admissible, the Whistleblowing Manager makes a primary assessment of the information provided in the Whistleblowing Report to ascertain its materiality, including:

- The rules, obligations conducts or standards allegedly violated;
- The underlying facts leading to reporting;
- The name, position and function of the persons allegedly responsible of the Reportable Concern;
- The name, position, and function of the Whistleblower (if applicable) and any other persons involved.

To comply with this obligation, the Whistleblowing Manager will complete a Whistleblowing Report follow-up form.

6. Internal investigation

The Whistleblowing Manager must act timely, with due diligence and take all available measures to conduct an internal investigation and remedy the reported breach (if any), whether the Whistleblowing Report is filed nominatively or anonymously.

The Whistleblowing Manager can interact at any time with the Whistleblower, as appropriate, to carry out this assessment.

The Whistleblowing Manager must provide, in any case, follow-up and feedback to the Whistleblower on actions or lack thereof within a reasonable timeframe, given the need to promptly address the problem that is the subject of the Whistleblowing Report.

Such timeframe should not exceed three (3) months but could be extended to six (6) months where necessary due to the specific circumstances of the case, in particular the nature and complexity of the subject of the Whistleblowing Report, which may require a lengthy investigation.

PART 6. EXTERNAL REPORTING

1. Reporting to the competent authority

The Whistleblower may share a Reportable Concern with a competent external regulatory body or authority, including criminal authorities, **provided that**:

- *After internal reporting*: they are not satisfied with the outcome of internal process – including if there has been no follow up to the internal reporting within the timeframe specified below; *or*
- *Directly, i.e. without internal reporting*: if they fear that their concern will not be addressed in a proper, independent and objective manner internally. The Whistleblower must however carefully examine the situation before deciding to file an external report directly, as internal reporting should always be preferred.

2. Public Disclosure

Whistleblowers are entitled to make a public disclosure[4] and qualify for the rights and protections laid in the Procedure **provided that**:

- The Whistleblower first reported the matter both internally and externally, or externally to the competent regulatory body or authority, but no appropriate action was taken in response to such reporting within the timeframe specified above **(PART 5**, **Section 3**); or
- The whistleblower has reasonable grounds to believe that:
  - The breach may constitute an imminent or manifest danger to the public interest, such as where there is an emergency or a risk of irreversible damage; or
  - In the case of external reporting, there is a risk of retaliation or there is a low prospect of the breach being effectively addressed, due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed or where an authority may be in collusion with the perpetrator of the breach or involved in the breach.

The Whistleblower must use the public disclosure channel as a means of **last resort, and only** provided that the above conditions are met.

Whistleblowers are aware that they may **lose** the rights and protections guaranteed in this Procedure in the event of a misuse of the public reporting channel[5].

PART 7. TRAINING

The Whistleblowing Manager is responsible for ensuring that Addressees are provided with adequate trainings on this Whistleblowing Policy, that they understand and are made aware of their duties, rights and protection as applicable.

Trainings must be provided on an ongoing basis, both when new employees are recruited and periodically as necessary.

Once every two years, the Whistleblowing Manager verifies that all Addressees have been trained adequately on this Whistleblowing Policy.

The Whistleblowing Manager makes periodic communications, as appropriate, to raise Adressees' awareness on this Whistleblowing Policy.

PART 8. RECORD KEEPING AND DATA PRIVACY

[4] I.e. through social networks, press release, public interviews or any other channel with similar effect.
[5] Whistleblowers who use public reporting channels compliance with this Procedure and Policy shall not be considered to have breached any restriction on disclosure of information and shall not incur any liability of any kind in respect of such public disclosure.

Gimv has implemented a whistleblowing register (the **Register**) to keep record of every report filed internally, whether admissible or not. This Register is operated under the control and supervision of the Whistleblowing Manager.

The Register records:

- The date and time of the report;
- The nature of the report;
- The rules, obligations conducts or standards allegedly violated;
- A summary of the underlying facts leading to the report;
- The name, position and function of the persons responsible of the breach;
- The name, position and function of the Whistleblower (if applicable);
- The function and position of other parties involved;
- The steps taken following-up to the filing of the report (as part of the investigation procedure);
- The conclusion on the veracity and materiality of the facts and Reportable Concern reported;
- The measures taken based on the conclusion of the investigation procedure;
- Any other relevant elements.

Records must be kept for five (5) years following the resolution of the matter.

Gimv ensures that all personal data collected further to this Whistleblowing Policy, including as part of any filing of a report, investigation and related procedure, are processed in respect of compliance of applicable data privacy law and obligations. This includes Regulation (EU) 2016/679 of 27 April 2016 (the GDPR) *and* the Belgian Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data, as well at Gimv's privacy policies**.**

Gimv also ensures that it provides the highest level of security in respect of the protection of sensitive data (if any).

PART 9. MONITORING AND IMPLEMENTATION OF THE PROCEDURE

1. Implementation

This Whistleblowing Policy has been approved by the Board of Directors. The Whistleblowing Manager has primary and day-to-day responsibility for ensuring the effective implementation of this Whistleblowing Policy.

2. Monitoring

The Whistleblower Manager must monitor the use and effectiveness of the Whistleblowing Policy on an ongoing basis, and review and update it as appropriate. Any improvements to the Whistleblowing Policy identified mut be made as soon as possible but at least on an annual basis. Comments, suggestions and queries regarding this Whistleblowing Policy must be addressed to the Whistleblowing Manager.

ANNEX 1: WHISTLEBLOWING REPORTING GUIDELINES FOR STAFF

If you want to voice a Reportable Concern to Gimv, please send your Whistleblowing Reports by email directly to the Whistleblowing Manager at the following address: compliance@gimv.com.

Please include at least the following details in your email for your Whistleblowing Report to be admissible:

- The underlying facts leading to the report, including but not limited to:
  - *The facts/events you witnessed or you suspect to have taken place*
  - *The circumstances in which the facts/events took place (setting, context, dates...)*
  - *Whether it is an ongoing misconduct/violation or a one-time event*
- The identity, functions and contact information of the persons subject of the report (i.e. the presumed wrongdoer);
- When reported nominatively, your identity, functions, and contact information.

Please also *attach* to your email any document substantiating and/or any supporting evidence of the Reportable Concern.

You must fully cooperate with and provide all relevant information requested by Gimv further to the filing of a Whistleblowing Report (if made nominatively) as well as throughout the internal investigation (if any).

You must always respect your duties of confidentiality and loyalty to Gimv in this context.

You are entitled to file your Whistleblowing Report anonymously. However note that, if you decide to remain anonymous:

- You will not receive any acknowledgment of receipt or feedback on your Whistleblowing Report;
- The Whistleblowing Manager will not be able to contact you to obtain additional information or supporting evidence to substantiate your report and the investigation (if any).

Please therefore make sure to provide as much specific and detailed information and supporting documentation as possible so as to allow the Whistleblower Manager to adequately assess the situation and follow up on your Whistleblowing Report.

ANNEX 3
GIMV DATA PROTECTION FRAMEWORK

GIMV DATA PROTECTION FRAMEWORK

Table of content

Table of content 2
1. Introduction 4
2. Scope 4
3. Definitions 4
4. Policy 5
4.1. Data protection 5
4.2. Responsible operators 6
4.3. Procedure 6
4.3.1. Phase 1: Monitoring 6
4.3.2. Phase 2: Investigation 7
4.3.3. Phase 3: Further actions in the event the investigation would show an unauthorised data processing or data leakage 7
4.4. Access rights in case of departure 7
4.5. Privacy 7
4.6. Questions and contact 8
5. Compliance 8
6. Reference documents 8

Title:	Gimv Data Protection Framework
Approved on:	16/05/2023
Version number:	2.0
Status:	Final
Owner:	Gimv Compliance Office

Policy reviewers

Name	Function
Bastijns Edmond	CLO
Creemers Johan	IT Manager
Dejonckheere Koen	CEO
Sellenslagh Laura	Paralegal & Compliance Assistant
Van Bueren Vincent	Corporate communications & ESG Manager
Vande Capelle Kristof	CFO

Policy version control

Version	Status	Date	Changed by	Description
1.0	Final	08/01/2018	Gimv	First publication.
2.0	Final	16/05/2023	Gimv, PwC	Review of policy.

1. Introduction

As a European listed private equity firm, Gimv has many different types of information in various forms, which are vital for its daily business activity and its position in the highly competitive private equity landscape. Gimv's most valued assets and most important ingredients for further sustainable growth today are:

i. its skilled and experienced employees;
ii. the interests in its portfolio companies; and,
iii. its valuable corporate (personal or non-personal) data, such as its data with respect to previous, current and potential portfolio companies and their management and employees, as well as data and/or information relating to the platform related markets (non-exhaustive examples).

Consequently, Gimv deems it necessary to implement all necessary organisational and technical measures to protect information and ensure the confidentiality, integrity and availability as well as resilience of the processing systems. Therefore, this document should be read in conjunction with the Gimv IT user policy[1].

The most important measure is creating a safe and highly secure IT environment, which mainly consists of:

i. security tools, such as firewalls, effective anti-virus software, back-ups, etc. and
ii. employees with prudent cyber activity behaviour and conscientiously handling information within the Gimv IT-environment (among others in accordance with the Gimv IT user policy[1]).

As an important closing piece of ensuring the protection of information and its information processing facilities and in application of article 10 of the Gimv Labour Standards, Gimv will monitor the way in which certain information are handled to prevent any unlawful or unauthorised data leakage or processing (hereafter the "Gimv Data Protection Framework" or "GDPF").

This framework has for main purpose to provide the Gimv employees of information processing facilities with some more information on GDPF (in line with Gimv's obligation to inform its employees on the processing of their personal data) and to address the privacy-related attention points attached thereto (including some very useful practical recommendations on employee behaviour in order to avoid information loss and facilitate the GDPF).

2. Scope

This policy applies to all Gimv employees or users (hereafter "employee"), regardless of their exact Labour Standard with Gimv, and to all external employees (e.g., contractors, interns, job students, …), who have lawful access to and use of information and/or information processing facilities of Gimv.

3. Definitions

In this document, the following verbal forms are used:

- "shall" indicates a requirement.
- "should" indicates a recommendation.

The table below highlights some definitions used in this document.

Definition	Description
Availability	Property of being accessible and usable on demand by an authorised entity.
Confidentiality	Property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
Data	Pieces of information from which "understandable information" is derived.
Information	Information is an asset that, like other important business assets, is essential to Gimv's business and, consequently, needs to be suitably protected. Information can be stored in many forms, including digital form (e.g., data files stored on electronic or optical media), material form (e.g., on paper), as well as unrepresented information in the form of knowledge of the employees. Information can be transmitted by various means including courier, electronic or verbal communication.
Information processing facilities	Any information processing system, service or infrastructure, or the physical location housing it.
Integrity	Property of accuracy and completeness.
Personal data	'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
User	Individual, or (system) process acting on behalf of an individual, authorised to access a system.

Table 1 - Definitions used in this policy.

4. Policy

4.1. Data protection

For the GDPF, Gimv will use the technical cloud solution 'DatAdvantage' developed by Varonis, an Israel based company in order to monitor file activity and user behaviour to protect Gimv confidential information against data breaches and other types of risks.

DatAdvantage monitors the handling of information by systematically logging the activity on and through 4 channels:

i. Gimv Active Directory (AD): monitoring who has access to what and when.
ii. Gimv central file servers: monitoring changes to internal files and file-content.
iii. Gimv mail servers: monitoring sender, receiver and subject of incoming and outgoing email correspondence.
iv. Gimv SharePoint: monitoring changes to files and file-content.

Gimv wishes to emphasise that the sole purpose of the GDPF is to uphold the integrity of the information. To that end, the usage of the four above mentioned central shared Gimv channels is monitored. To avoid any doubt, any other individual employee behaviour such as surfing activity or mobile communication is not monitored.

DatAdvantage is an off-the-shelf solution, which will run on premise at Gimv (Antwerp, Belgium) for the monitoring of the information in Belgium, France, Germany and the Netherlands. Varonis as provider will by default not store or otherwise process (personal) data on its own behalf or on behalf of Gimv. The data collected by DatAdvantage will be stored at Gimv (Antwerp, Belgium) for a period of two (2) years as of the date of the monitoring, whereby specific data may be stored for a longer period, if necessary, in the context of a GDPF Phase 2 (see below).

4.2. Responsible operators

The GDPF will be jointly operated by the Gimv Compliance Office (the "Responsible Operators").

4.3. Procedure

The monitoring of the way in which certain information are handled will be carried out in a step-by-step procedure, in order to guarantee that the privacy of employees is only intruded to the minimum extent possible.

In short, the continuous and automatic monitoring occurs in first instance on a high level and statistical basis in the background of our IT environment (hereafter "**Phase 1**"), whereby DatAdvantage will flag to the Responsible Operators anomalous behaviour with respect to information, such as copying high volumes of information on external hard drives or USB flash drives or redirecting emails to private or personal email accounts on a regular basis (non-exhaustive examples) without directly identifying the employee(s) involved in such behaviour.

If such anomalous behaviour is flagged, the Responsible Operators verify whether a further investigation of the anomalous behaviour is necessary.

Only in the investigation phase (hereafter "**Phase 2**"), individualisation of the employee(s) involved will take place. If and when the Responsible Operators encounter data, information or correspondence which at first sight appear to be of a non-professional nature (see practical recommendations below), they will first only be consulted by the Gimv Compliance Office (acting as trusted intermediary) to assess whether these are relevant for the investigation, as the case may be in presence of the concerned employee unless such would harm the investigation.

The Responsible Operators will ensure that during each investigation, the compliance with the foreseen step-by-step approach and other measures as well as the decision process is duly documented in a report to the Gimv Compliance Office. Such reports are securely stored by the Gimv Compliance Office for maximum 5 years, unless the investigation would show an unauthorised data processing or data leakage in which case Gimv will keep the Report and necessary Gimv information as long as needed to safeguard and protect its legal interest.

4.3.1. Phase 1: Monitoring

The Gimv IT Manager (with the Gimv Compliance Office as back up) will daily manage Phase 1 of the GDPF and will review the anomalous behaviour flagged by DatAdvantage on a high level and statistical basis. When during Phase 1 anomalous behaviour is detected, the Gimv IT Manager will immediately alert and consult with the members of the Gimv Compliance Office. Based on the nature of the detected anomalous behaviour, the Gimv IT Manager and the Gimv Compliance Office will jointly decide whether to proceed with Phase 2 or not.

4.3.2. Phase 2: Investigation

If and when Phase 2 is started, the Gimv Compliance Office will appoint one of its Responsible Operators to further investigate the detected anomalous behaviour together with the Gimv IT Manager to ensure a 4-eye review by a trusted intermediary. They will proceed with the individualisation of the employee(s) involved and further investigate the case at hand. Two situations might arise at this stage:

i. If no data, information or correspondence that at first sight appear to be of a non-professional nature (for instance because of the mentioning of 'PRIVATE', 'PRIVE' or 'PERSONAL' in the subject field, the nature of the subject, the recipient; non-exhaustive examples), are encountered during this investigation, the investigation will be further handled and concluded by a report to the Gimv Compliance Office.
ii. If data, information or correspondence that at first sight appear to be of a non-professional nature, are encountered during this investigation and are suspected to be relevant for the investigation, the Gimv Compliance Office (acting as trusted intermediary) will first analyse such data, information or correspondence to assess whether these are indeed relevant. Where possible, the Gimv Compliance Office will invite the employee or concerned individual to be present during such analysis, unless such presence would harm the investigation in which case the Gimv Compliance Office will document and duly motivate its decision and include such decision in the investigation report.
    - In case the Gimv Compliance Office confirms the relevance of the data, information or correspondence, the investigation will be further handled by the Responsible Operators and concluded by a report to the Gimv Compliance Office.
    - If not, the data, information or correspondence is not further investigated.

4.3.3. Phase 3: Further actions in the event the investigation would show an unauthorised data processing or data leakage

Upon receipt of the report with the conclusions of Phase 2, the Gimv Compliance Office will further notify and enter into dialogue with the employee(s) involved, if necessary or appropriate together with their responsible manager(s). Hereafter, the Gimv Compliance Office in consultation with the responsible manager(s) of the employee(s) involved will advise on any consequences, measures or next steps to be taken (see 5. Compliance).

4.4. Access rights in case of departure

In case of (voluntary or forced) departure of a Gimv employee, the Gimv Compliance Office will decide on the further management of access rights of the employee concerned during the time they are still operative at Gimv[1].

Please note that in case of both voluntary and forced departure, the Gimv Compliance Office will handle and judge all requests on receiving certain information upon departure in mutual consultation with the employee concerned. As such, there is no need for any hasty copying or emailing information to your personal email account or external drives.

4.5. Privacy

As the GDPF will monitor the way in which certain information are handled, it will also bring about the monitoring of the cyberactivity of the Gimv employee(s) when using the abovementioned 4 channels (see chapter 4.1. Data protection), including the processing of their personal data (e.g. (electronic) identification data and professional data).

Gimv will process its employees' personal data in this respect on the basis of its legitimate interest to protect the information (as explained above), however continuously ensuring and balancing the processing activities with the fundamental privacy rights of its employees and

implementing a monitoring which is transparent, adequate, relevant, necessary and not excessive in respect of its finality (as further elaborated above).

In particular, Gimv has taken the following organisational and technical measures (as further elaborated above) in order to ensure the privacy of employees is only intruded to the minimum extent possible:

i. A multi-phase procedure whereby the continuous monitoring in first instance takes place on a high level and statistical basis only and individualisation of the employee(s) involved only occurs if needed and in a later phase (i.e., when appropriate and necessary in the context of the purpose of the GDPF).
ii. The detection of anomalous behaviour in Phase 1 does not necessarily lead to an investigative Phase 2. The Gimv Compliance Office and the Gimv IT Manager, jointly make a case-by-case assessment of whether Phase 2 should be initiated. As such, there is no automated decision-making.
iii. A four-eye principle is fitted into the procedure to assure that the individualisation of the employee involved is done in a proper way, and that the privacy of each employee is respected to the extent possible taking the purpose of the GDPF into account.

4.6. Questions and contact

In case of any questions with respect to the GDPF, please do not hesitate to contact the Gimv Compliance Office (compliance@gimv.com) or Johan Creemers, Gimv IT Manager (johan.creemers@gimv.com).

Under certain conditions, you have the right to request access to, rectification of, erasure of or portability of your personal data, as well as to request restriction of processing, to object to processing or to lodge a complaint with the Belgian Privacy Commission. If you would like to exercise these rights or have any questions in this respect, please do not hesitate to contact the Gimv Compliance Office (compliance@gimv.com). More information with respect to your privacy rights can also be found on the website of the Belgian Privacy Commission (www.privacycommission.be).

5. Compliance

Prohibited use, as described in this policy is sanctioned in accordance with the applicable provisions. Depending on the case, the sanction will range from a simple warning or to a more severe sanction in accordance with the work regulations and/or national law.

6. Reference documents

Ref.	Document
[1]	Gimv IT user policy

ANNEX 4
GIMV EXPENSE POLICY

Gimv Expense policy – November 2019

1. Purpose

The purpose of this policy is to define rules for employees of Gimv Group seeking to reclaim expenses incurred in the context of their professional activities. All expenses incurred in the context of professional activities for Gimv are eligible for reimbursement following approval by Finance and the employee's manager. Specific rules apply for the Belgian employees who receive a fixed monthly expense allowance. Gimv Finance is responsible for drafting this policy, monitoring the follow-up and keeping it up to date.

2. Procedure

Each Gimv employee is allowed to reclaim expenses by following the standard procedures. An expense item has to be registered in Scansys, either via the mobile application or via the Scansys web portal. One or more expense items can be grouped into one expense note which can be submitted for approval (a detailed guide how to group expense items can be found on the Gimv intranet). For each expense item, correct and detailed business justification should be provided.

The expense claim must be submitted within 2 months after incurring the expense. When preparing the expense item, evidence (see 6. Supporting documents) must be attached in order to be reviewed by the approvers.

Gimv Finance is responsible for paying the approved expense notes within two weeks after approval. Finance and HR should be alerted in case of change in the employee's bank account. The requestor will be notified if his or her expense claim is rejected.

3. Company credit cards

Each staff member is entitled to a company credit card. The request for a company credit card will be managed by Gimv Finance. All expenses financed with the company credit card are billed to and settled by Gimv, the cardholder does not need to prefinance.

The expenses with the company credit care will be uploaded to the Scansys portal on a regular basis (at least once per month). To prove the eligibility of the expenses, each cardholder has to link each imported credit card item with a created expense item including the supporting documents.

Company credit cards may not be used to withdraw cash.

Personal expenses may not be financed with the company credit card. In the exceptional case that the company credit card was used for personal expenses, please inform Gimv Finance asap. Either Gimv will issue an invoice to the employee, or the employee must create a negative expense item (financed with own resources) for the amount of the personal expense.

4. Approval

The expense claims go through an automatic and digital approval process. Each submitted expense note will be reviewed by Finance who will first check that the expense claim is in line with this policy. After

approval of Finance, the expense note will be sent to the approver (platform head or budget owner). The approver must check that the claimed expenses have been incurred in the context of professional activities and that they comply with this policy.

Please remind that a budget owner may not be the final approver of any claim of an expense incurred during an event where he was present.

5. Compliance & Escalation procedure

All employees are responsible for complying with this policy. Regular non-compliance will result in disciplinary actions (potentially including the withdrawal of the company credit card). Non-compliance can for instance be the absence of supported documents, personal expenses financed with the company credit card without informing Finance, late registration and submission of expense notes, etc.

6. Supporting documents

Each submitted expense item, either financed with own resources or with the prepaid company credit card, must be accompanied with a picture or scanned version of the original receipt. The employee is obliged to retain the original receipt until the submitted expense note has been approved. All supporting documents are stored in the database and will be available for submission in case of any tax audit.

An adequate supporting document is a clear picture of the expense ticket. A picture of the payment confirmation without any detail is not sufficient.

7. Fixed Allowance

Belgian Gimv Employees receive a monthly fixed allowance. This allowance covers the following expenses:

- Expenses associated with office space at home (internet, printer, ink cartridges, etc);
- Call charges and subscription costs of private landline or mobile internet connection;
- Small expenses during company travel abroad (drinks, snacks, etc), to a maximum of EUR 5,00
- Parking fees and public transport to a maximum of EUR 5,00
- Car wash

These expenses cannot be reclaimed by the Belgian Gimv employees.

8. Recharge to a third party

In case expenses need to be recharged to a third party, the employee must indicate the recharge option while registering the expense item. More detail of the third party must be entered in the available text box. Gimv finance will be alerted to recharge the expenses only if the recharge option is set at ‘yes’.

9. What expenses are eligible?

1) Kilometer compensation

Business kilometers with a private car are eligible for reimbursement if you do not have a company car with fuel card. The home – work distance is not considered as business kilometers. Business justification should be provided when claiming the payment for the use of the private car.

The rate used for the reimbursement differs per country, below the current rate for employees in:

Belgium:	EUR 0,3653 per km
Germany:	EUR 0,3000 per km
The Netherlands:	EUR 0,1900 per km
France:	depends on multiple factors

2) Fuel costs

Employees with a company car are entitled to a fuel card. The fuel card can be used in most of the European countries (also for private use). An overview of the fuel brands included in the network (per country) can be retrieved on the fuel card's website or via simple request to the Gimv fleet responsible.
Each refueling must be paid with the fuel card. In the exceptional case the fuel card has been lost, doesn't function or is not yet available, company car users can reclaim their fuel costs financed with own resources or the company credit card.

It is not allowed to pay the car wash on the property of the gasoline station with the fuel card. The payment of toll expenses or ferries or similar transport expenses for private reasons is also not allowed.
It goes without saying that the fuel card is only to be used to refuel your own company car.

The fleet responsible and Gimv Finance will monitor the fuel card expenses on a regular basis to make sure that the use of the fuel card complies with this policy.

3) Other car expenses

Parking expenses

Parking expenses are eligible expenses. Parking fines and retributions on the other hand are not eligible.

Car wash

Car wash expenses are eligible expenses except for Belgian employees (included in allowance).

Car Inspection

This covers the costs incurred for a technical inspection of your company car. Car inspection expenses are eligible expenses.

Garage costs

Garage costs for the company car are in principle always invoiced directly by the garage to the leasing company. In exceptional cases (e.g. urgent and necessary intervention by a garage that does not have a cooperation agreement with the leasing company), the garage can invoice the driver concerned directly. The driver can in turn reclaim the garage costs by means of an expense item.

Replacement car
Most lease agreements will include a replacement car in case the company car is immobilized for more than 24 hours. In that case the invoice for the replacement vehicle will be paid by the lease company.

In case a replacement car is needed within the time frame of 24 hours, the replacement car cost is an eligible expense that will be reimbursed.

4) Hard- and software expenses

All IT equipment and accessories needed for professional use have to be requested through (after approval by the manager) or approved by the IT department and cannot be part of expense claims. The purchase of any accessory to protect the Gimv IT material (eg. phone covers) cannot be reclaimed.

5) Professional literature

It is allowed to reclaim expenses with regard to professional literature, however we encourage to purchase literature via invoice. The goods remain the property of Gimv.

6) Meals, drinks and restaurant expenses

Restaurant charges with existing or potential investment targets or with business contacts are eligible expenses.

Meals with Gimv colleagues only are excluded from reimbursement, except as part of team events or during company travel abroad. The name of the team event or the reason for the company travel abroad must be mentioned in the expense item.

In order to comply with social and fiscal law, any eligible restaurant charge must be submitted including additional details such as the number of invited participants and the reason of the expense.

7) Travel expenses

As a general rule, all expenses related to business travel can be reclaimed (excl. some exceptions for Belgian employees cfr. supra). Please consider alternatives like telephone or video conferences when applicable.

All requests for business travel must be made using the preferred travel agency of the respective Gimv office through the assistants.

Air travel
Travelers are encouraged to book economic sensible rates. Early bookings are encouraged. Business class is only acceptable on business trips with an uninterrupted flight duration of more than 6 hours. Expenses incurred as a result of delay are eligible expenses (for instance overnight stay).

Railway travel
We encourage to book train tickets in advance through the preferred travel agency of the respective Gimv office. Travelers are allowed to reserve business rate tickets.

Taxi and public transport

Taxi expenses and public transport means are eligible expenses. Any tip paid will be reimbursed subject to a proof of payment.

Hotel accommodation

Travelers are encouraged to book hotel rooms at economic sensible rates. Hotels with up to a 4-star rating are allowed. We encourage to book hotels via the preferred travel agency of the respective Gimv office. Online reservations (e.g. via booking.com) are also allowed.

Car Hire

Travelers can rent a car (economic class) if there are no other ways of transport available.

Passports and Visas

Passports and their validity are the responsibility of the traveler. Gimv will not reimburse the cost of a new or replacement passport.

Cancellation of bookings / changes to bookings

For changes to journeys for which tickets have already been purchased, we encourage to contact the travel agency of the respective Gimv office.
Amending tickets in case of changes to journeys are often expensive and should be restricted to a minimum.

ANNEX 5
GIMV IT USER POLICY

GIMV IT USER POLICY

Table of content

1. Introduction 4
2. Scope 4
3. Definitions 4
4. Policy 5
   4.1. Acceptable use of assets 5
   4.2. Installation of software 5
   4.3. Controls against malicious activities 6
   4.4. Accounts and user credentials 6
   4.5. Secure transfer of information 6
   4.6. Travel and teleworking 7
   4.7. Physical security 7
   4.8. Use of Artificial Intelligence 7
   4.9. Information security awareness, education and training 8
5. Compliance 8
6. Reference documents 8

Title:	Gimv IT user policy
Approved on:	13.01.2026
Version number:	5.1
Status:	Final
Owner:	IT department

Policy reviewers

NAME	FUNCTION
Bastijns Edmond[1]	CLO – Secretary General
Creemers Johan	IT Manager
Sellenslagh Laura	Compliance Associate
Van Bueren Vincent	Corporate Communications & Sustainability Director
Vande Capelle Kristof[2]	CFO

Policy version control

VERSION	STATUS	DATE	CHANGED BY	DESCRIPTION
0.1	Draft	26/03/2013	Kristof Poppe	Adapted to first review.
1.0	Final	18/06/2013	Kristof Poppe	Extended with general IT info.
2.0	Final	13/11/2014	Kristof Poppe	Updated on current setup.
3.0	Final	21/11/2014	Kristof Poppe	General update and extension.
4.0	Final	16/01/2018	Kristof Poppe	Updated release.
5.0	Final	16/05/2023	Gimv, PwC	Review of policy.
5.1	Final	13/01/2026	Gimv	Operational improvements and updated with a governance on the use of AI.

[1] On behalf of Edmond Bastijns BV
[2] On behalf of Hawoka BV

1. Introduction

The purpose of this policy is to clarify the responsibilities of all users of the information systems of Gimv to ensure the confidentiality, integrity and availability of Gimv information and information processing facilities. This document outlines possible steps that may be considered if these users are not compliant with the guidelines as set out in this policy (see 5. Compliance).

2. Scope

This policy applies to all persons who have access to or are authorized to use the IT infrastructure of Gimv, regardless whether they are employees, self-employed, acting through a management company, interns, job students, contractors or other (hereafter the "User").

3. Definitions

In this document, the following verbal forms are used:

- "shall" indicates a requirement.
- "should" indicates a recommendation.

The table below highlights some definitions used in this document.

DEFINITION	DESCRIPTION
Artificial Intelligence (hereafter "AI")	Technologies that fall under the definition of an 'AI system' in the EU AI Act (Regulation (EU) 2024/1689) (hereafter "EU AI Act"), which refers to systems using machine-based methods to produce outputs like predictions, recommendations or decisions.
Availability	Property of being accessible and usable on demand by an authorised entity.
Confidentiality	Property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
Data	Pieces of information from which "understandable information" is derived.
Information	Information is an asset that, like other important business assets, is essential to Gimv's business and, consequently, needs to be suitably protected. Information can be stored in many forms, including digital form (e.g., data files stored on electronic or optical media), material form (e.g., on paper), as well as unrepresented information in the form of knowledge of the Users. Information can be transmitted by various means including courier, electronic or verbal communication.
Information processing facilities	Any information processing system, service or infrastructure, or the physical location housing it.
Information security event	Identified occurrence of a system, service or network state indicating a possible breach of this Gimv IT user policy or failure of controls, or a previously unknown situation that can be security relevant.
Information security incident	Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
Information system	Set of applications, services, information technology assets, or other information-handling components.

Integrity	Property of accuracy and completeness.
IT device	All types of computers, tablets, phones and other Gimv devices.
Remote wipe	This option removes all data and applications from the IT device and brings the device back to its manufacture state.
Person	Individual, or (system) process acting on behalf of an individual.

Table 1 - Definitions used in this policy.

4. Policy

4.1. Acceptable use of assets

4.1.1 All IT devices and information stored on electronic and computing devices provisioned to the User remains property of Gimv and should primarily be used in the context of the execution of this policy and any other arrangement agreed between Gimv and the User.

4.1.2 The User undertakes proper and responsible use of the IT devices and keeps it in good working condition, always, as if it was their private property, respecting its nature and purpose.

4.1.3 The User should only use IT devices provided by Gimv or validated by Gimv to access company networks.

4.1.4 Users shall be aware that Gimv monitors the IT infrastructure for lawful purposes, to protect the availability, integrity and confidentiality of information (systems) and information processing facilities[1].

4.1.5 In the event of an IT device being lost or stolen, the User shall inform the IT department[2], giving details of the circumstances of the loss or theft and the confidentiality of the business information stored on it. Gimv reserves the right to remotely wipe the IT device where possible as a security precaution. They may involve the deletion of non-business data belonging to the owner of the IT device.

4.1.6 The User shall upon request by the IT department return the IT device at any time for inspection and/or audit.

4.1.7 The User shall upon leaving Gimv, depending on the agreement with the User, return or keep all provided IT devices and allow the IT department to remove all business data and applications from the IT devices.

4.1.8 The User shall not remove any identifying marks on the IT device such as a company device tag or serial number.

4.2. Installation of software

4.2.1 The User shall only install licensed software provided by the IT department and shall therefore not duplicate, reproduce, or install software on more than one IT device. All installations of software shall be performed under control of/or by the IT department[2].

4.2.2 The User shall keep the IT devices updated at all times.

4.2.3 The User should inform the IT department if a software application is no longer required. The software will then be removed from the IT device in question and where possible the licence will be re-used elsewhere within Gimv.

4.2.4 The User shall only install applications for mobile IT devices from official App Stores like Apple's App Store, Google Play, Windows Phone store, etc.

4.2.5 The User shall not download illegal, unvalidated software and/or videogames on IT devices provided by Gimv. This includes evaluation versions of software programs unless explicitly approved by the IT department.

4.2.6 The User shall not distribute, change or delete software provided by Gimv.

4.3. Controls against malicious activities

4.3.1 The User shall immediately report any suspected information security event or incident to the IT department.

4.3.2 The User shall not change (security) configuration settings, bypass or subvert system security controls or to use IT devices for any purpose other than intended (e.g., disabling antivirus software, “rooting” or “jail-breaking”).

4.3.3 The User shall not make changes to system settings that prevent system updates from being installed.

4.3.4 The User shall not open files or attachments from an unknown, suspicious or untrustworthy source when there is reason to believe the content may compromise any of Gimv’s information systems or integrity.

4.4. Accounts and user credentials

4.4.1 The User shall always use a password or Personal Identification Number (PIN) to protect IT devices from unauthorised access.

4.4.2 The User shall change password upon first use.

4.4.3 The User shall protect their own username and password provided by the IT department and avoid keeping records (e.g., on paper, software file or hand-held device). Gimv recommends using a password vault (e.g., Heylogin[2]) to keep user credentials secure. Please contact the IT department for recommended password vault applications.

4.4.4 The User shall only use own username and password to login to information systems of Gimv and is strongly discouraged from sharing passwords with others (incl. staff, third parties or the IT department), unless there is a clearly justified and necessary reason to do so.

4.4.5 The User shall adhere to the minimal set of requirements when creating a new password[2].

4.4.6 The User shall inform the IT department or their platform head(s) / responsible manager(s) of any changes to their role and access requirements.

4.4.7 The User shall notify the IT department when the confidentiality of secret authentication information was or is thought to be compromised (see also 4.3.1).

4.4.8 The User should not use their business account for private purposes (e.g., use business credentials for LinkedIn) or use business credentials for private purposes, unless internally agreed upon with their platform head(s) / responsible manager(s) in a specific context.

4.4.9 The User should not enter login details when others are watching (i.e., “shoulder surfing”).

4.4.10 The User should not use the “remember password” feature in a browser unless it is the extension from a password vault.

4.4.11 The User should not re-use the same password for multiple accounts.

4.5. Secure transfer of information

4.5.1 The User shall protect any confidential information sent, received, stored or processed, including both electronic and paper copies. To share confidential information, contact the IT department or their platform head(s) / responsible manager(s) e.g., to set up Microsoft Teams[2] for the safe and secure transfer of (confidential) information.

4.5.2 The User should use appropriate security methods (e.g., encrypt Excel files and send password via SMS) when sending confidential information over the Internet via email. In case of questions please contact the IT department.

4.5.3 When leaving Gimv, the User shall inform their platform head(s) / responsible manager(s) prior to departure of any important information held in their account[1].

4.5.4 The User should always verify the correct recipient email address(es) are entered when sending emails so that confidential information is not compromised.

4.5.5 The User should securely store confidential printed material (i.e., clean desk) and ensure it is correctly destroyed when no longer needed.

4.5.6 The User should collect printed documents immediately from the printer and use the secure print function[2] where possible.

4.5.7 The User should in principle not use their own private email address for business purposes or vice versa (for example, sending confidential information from a private email address). Forwarding email to personal mailboxes is not allowed, unless there is a clearly justified and necessary reason to do so.

4.5.8 The User should not send confidential information to an insecure, unattended printer where it may be seen or picked up by unauthorised people. Where necessary, use the secure print function[2] where possible.

4.5.9 Prior to sending information to third parties, not only should the intended recipient be authorised to receive such information, but the procedures and information security measures adopted by the third party shall be considered to assure the confidentiality and integrity of the information.

4.5.10 The User should never store confidential information in public or private cloud services. If in doubt, please contact the IT department (see also: 4.5.1).

4.6. Travel and teleworking

4.6.1 When using public networks assume that the network is not secure. It is recommended to connect via your iPhone's personal hotspot. Keep the following recommendations in mind:

i. Avoid accessing confidential information.
ii. Only connect to "HTTPS" websites.
iii. Use a privacy screen (see also: 4.6.5).
iv. Use two-factor authentication.
v. Keep your operating system (OS) up to date.
vi. Use antivirus software.
vii. Remember to logout and do not enable auto-login.

4.6.2 The User should terminate active sessions by locking their screen (i.e., clear screen) when leaving the workplace to prevent unauthorised access to information via their account.

4.6.3 The User should protect IT devices and confidential information from physical access by unauthorised persons by using lockers, lockable cabinets to store confidential information and ensure the key is not easily accessible.

4.6.4 The User should destroy printed documents containing confidential information using available methods, such as a shredder.

4.6.5 The User should be aware of their surroundings when working in public places, to ensure unauthorised people cannot view or take photographs or video of the screen (i.e., shoulder surfing).

4.6.6 The User should use Gimv guest network when using mobile phones or privately owned IT devices.

4.6.7 When travelling by plane the laptop shall be kept in the carry-on luggage.

4.6.8 The User should not leave IT device(s) and badge unattended in view in public areas such as in the back of a car, in a meeting room or hotel room/lobby, etc.

4.7. Physical security

4.7.1 The User should remain vigilant regarding the presence of visitors, and ensure that access to Gimv premises is appropriate and consistent with internal security expectations. For secure areas, the User should accompany visitors when reasonably necessary.

4.8. Use of Artificial Intelligence

4.8.1 The User shall exercise due care when using AI, thereby safeguarding the integrity of Information and in alignment with the principles of the EU AI Act, as further explained in paragraphs 4.8.2 through 4.8.5.

4.8.2 The User shall never make use of AI in ways that could result in bias, discrimination or unfair treatment of individuals or groups.

4.8.3 The User shall not use public or externally hosted AI to process sensitive, personal or confidential information, unless there is a GDPR- compliant data processing agreement in place with the AI tool provider, (i) implementing appropriate technical and organizational measures to protect data; and (ii) providing sufficient guarantees regarding the processing, storage and transfer of personal data. All use of AI must comply with this policy and the Gimv Data Protection Framework. In case

of uncertainty regarding the existence or adequacy of a data processing agreement, the User shall consult the IT team to ensure proper alignment and compliance prior of the use of AI.

4.8.4 The User should disclose the use of AI in drafting materials or data analysis when it is relevant to the specific case or context, particularly when the AI-generated content is used substantially or without significant modification.

4.8.5 The User shall remain responsible for the output of the use of AI, as AI does not replace human judgement. The User shall always critically review all AI-generated output, before it's use.

4.8.6 The User should consult the Gimv AI Shortlist[3], which maintains an inventory of approved AI tools within Gimv that involve the use of sensitive and confidential information. These tools are reviewed and approved by the IT team, considering compliance, security and ethical standards. Users are encouraged to consult the IT team before using any AI tools that are not included on the Gimv AI Shortlist.

4.9. Information security awareness, education and training

4.9.1 The User shall comply with legal, statutory and contractual obligations as well as be familiar with the Gimv IT data protection framework[1] and procedures and any special instructions relating to their work.

4.9.2 The User shall follow trainings (such as phished.io trainings) provided by the IT team if and when made available.

5. Compliance

Prohibited use, as described in this policy is sanctioned in accordance with the applicable provisions. Depending on the case, the sanction will range from a simple warning or to a more severe sanction in accordance with the work regulations and/or national law.

6. Reference documents

REF.	DOCUMENT
[1]	Gimv Data Protection Framework
[2]	See Gimv Portal for the specific procedure.
[3]	Gimv AI Shortlist