CODE OF CONDUCT

Date of Issuance: 20 September 2016
Date of Most Recent Update: 21 June 2022

Gimv NV
Karel Oomsstraat 37, 2018 Antwerp, Belgium
T +32 3 290 21 00 | **F** +32 3 290 21 05
www.gimv.com

1 TABLE OF CONTENTS

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

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

1) Why?

As a European listed private equity firm, Gimv has many different types of data 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 relating to the platform related markets (non-exhaustive examples) (hereafter "**Gimv-data**").

Consequently, Gimv deems it necessary to implement all necessary organizational and technical measures to protect the Gimv-data and ensure the confidentiality, integrity and availability as well as resilience of the processing systems. 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 a prudent cyber activity behavior and conscientiously handling the data within the Gimv IT-environment (among others in accordance with the Gimv IT Policy).

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

This policy has for main purpose to provide the Gimv employees and other users of Gimv data processing systems 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 behavior in order to avoid data loss and facilitate the GDPF).

2) How?

For the GDPF, Gimv will use the technical solution 'Datadvantage' developed by Varonis, an Israel based company that gives organizations more visibility into their data and how to protect their critical information.

Datadvantage will monitor the handling of Gimv-data by systematically logging the activity on and through 4 channels:

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

Gimv wishes to emphasize that the sole purpose of the GDPF is to uphold the integrity of the Gimv-data. To that end, the usage of the 4-abovementioned central shared Gimv channels is monitored. To avoid any doubt, any other individual employee or user behavior such as surfing activity or mobile communication is <u>not</u> monitored.

Datadvantage is an off-the-shelve solution, which will run on premise at Gimv (Antwerp, Belgium) for the monitoring of the Gimv-data 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).

3) Responsible operators

The GDPF will be jointly operated by the Gimv IT Manager and the Compliance Manager within the Gimv Compliance & ESG Office (the "**Responsible Operators**").

4) Procedure

The monitoring of the way in which certain Gimv-data 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 Gimv IT Manager anomalous behavior with respect to Gimv-data, such as copying high volumes of data 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 behavior.

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

Only in the investigation phase (hereafter "**Phase 2**"), individualization of the employee(s) involved will take place. If and when the Responsible Operators encounter data, documents 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 & ESG 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 or user 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 & ESG Office. Such reports are securely stored by the Gimv Compliance & ESG Office for maximum 5 years, unless the investigation would show an unauthorized data processing or data leakage in which case Gimv will keep the Report and necessary Gimv data as long as needed to safeguard and protect its legal interest.

Phase 1: monitoring

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

Phase 2: investigation

If and when Phase 2 is started, the Gimv Compliance & ESG Office will appoint the Compliance Manager or any of its other members to further investigate the detected anomalous behavior together with the Gimv IT Manager to ensure a 4 eye review. They will proceed with the individualization of the employee(s) involved and further investigate the case at hand. Two situations might arise at this stage:

- If no data, documents 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 & ESG Office.

- If data, documents 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 & ESG Office (acting as trusted intermediary) will first analyze such data, documents or correspondence to assess whether these are indeed relevant. Where possible, the Gimv Compliance & ESG 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 & ESG Office will document and duly motivate its decision and include such decision in the investigation report.

    - In case the Gimv Compliance & ESG Office confirms the relevance of the data, documents or correspondence, the investigation will be further handled by the Responsible Operators and concluded by a report to the Gimv Compliance & ESG Office.

    - If not, the data, documents or correspondence is not further investigated.

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

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

5) Access rights in case of departure

In case of (voluntary or forced) departure of a Gimv employee or user, the Gimv Compliance & ESG Office will decide on the further management of access rights of the employee or user concerned during the time that he/she is still operative at Gimv.

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

6) Privacy

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

Gimv will process its employees' or other users' personal data in this respect on the basis of its legitimate interest to protect the Gimv-data (as explained above), however continuously ensuring and balancing the processing activities with the fundamental privacy rights of its employees or other users 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 organizational and technical measures (as further elaborated above) in order to ensure the privacy of employees or concerned users is only intruded to the minimum extent possible:

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

i.

7) Some practical recommendations

The current Gimv labour and policy framework allows for personal and private email communication via your Gimv email account (although limited). In order to facilitate the GDPF and avoid that personal and private emails or data are mistakenly perceived as professional emails, we strongly recommend the Gimv employees to:

(i) limit such personal and private email communication and use by preference your private email account for these purposes;

(ii) indicate, when sending personal and private email communication via your Gimv email account, that it concerns personal or private communication by for instance mentioning 'PRIVATE', 'PRIVE' or 'PERSONAL' in the subject field. Abusing this method to cover any illegitimate behavior is not tolerated off course and may cause disciplinary consequences; and

(iii) not to store personal or private data within the Gimv IT-environment.

Furthermore, we strongly recommend the Gimv employees or users of Gimv data processing systems to make use of all shared servers and spaces within the Gimv IT-environment which are at the continuous disposal of all Gimv employees. These servers and spaces are managed and maintained by the Gimv IT-department and back-ups thereof are made on a regular basis to avoid data losses.

Finally, we strongly advise Gimv employees to limit as much as possible the use of external hard drives or flash/USB drives. There are numerous ways to log on the protected Gimv virtual desktop environment (VDI) with full access to the Gimv-data. As such, there is no need to create parallel working environments outside the highly secure Gimv IT environment.

If and when the GDPF shows extensive and/or systematic unlawful data leakages, Gimv preserves the right to prohibit temporarily or indefinitely any use of such external hard drives or flash/USB drives or any non-professional use of the Gimv email account and/or the Gimv IT-environment.

8) Questions and contact

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

ANNEX 4
GIMV EXPENSE POLICY

ANNEX 5
GIMV IT-POLICY