Gimv

CODE OF CONDUCT

Date de publication : 20 septembre 2016
Date de mise à jour la plus récente : 16 mai 2023

1 TABLE DES MATIERES

2 INTRODUCTION ET PORTEE

2.1 PORTEE

Le présent ***Code of Conduct***, tel qu'approuvé par le Conseil d'Administration de Gimv, est applicable à chaque employé (y compris les intérimaires et les stagiaires) de Gimv et de ses filiales (un « ***Employé*** »), ainsi qu'à chaque membre du conseil d'administration de Gimv (un « ***Administrateur*** ») (l'Employé et l'Administrateur sont dénommés ci-après conjointement « ***Destinataire*** »). Pour éviter toute ambiguïté, les filiales ne comprennent en aucune manière les sociétés en portefeuille externes de Gimv ni la coentreprise d'infrastructure Gimv-Belfius TDP, TINC et les fonds gérés par TDP.

Le présent Code of Conduct fournit des orientations générales importantes. Il ne s'agit toutefois pas d'un document exhaustif anticipant chaque situation qu'un Employé ou un Administrateur pourrait rencontrer dans ses activités journalières. Gimv attend des Destinataires qu'ils agissent toujours de manière responsable et consciencieuse. Si un Destinataire a des questions ou un doute sur les dispositions du Code of Conduct ou s'il se demande si un acte va à l'encontre des dispositions ou de l'esprit du Code of Conduct, Gimv conseille à ce Destinataire de contacter immédiatement le Gimv Compliance & ESG Office.

Le Code of Conduct porte sur (i) les interactions avec les sociétés en portefeuille (la négociation des actions de sociétés en portefeuille et la réception de rémunérations pour des missions dans des sociétés en portefeuille), (ii) l'établissement d'une norme en tant qu'Employé ou Administrateur de Gimv en matière de respect et d'intégrité, et (iii) la communication au public. Certains principes du code de conduite sont précisés par des politiques ou des procédures spécifiques. À ce titre, le Gimv Whistleblowing Policy, le Gimv Data Protection Framework, le Gimv Expense Policy et le Gimv IT-policy sont ajoutés en tant qu'annexes au Code of Conduct et sont considérés comme faisant partie intégrale de celui-ci. Pour les règles internes applicables aux Négociations d'Actions de Gimv, nous nous référons au Gimv Dealing Code, qui est distinct.

Le Code of Conduct reflète certains principes fondamentaux qui ont une grande valeur pour Gimv, ainsi que les politiques ou procédures que les Destinataires doivent respecter. Toutefois, le Code of Conduct ne confère aucun droit à aucun gouvernement, actionnaire, Société en Portefeuille, fournisseur, concurrent ou toute autre personne ou entité.

Le Code of Conduct et ces annexes peuvent être soumis à des mises à jour et des modifications découlant des nouvelles lois et réglementations ou des évolutions significatives au sein de la société. Tous les Destinataires seront informés par e-mail de toute modification apportée à ce Code of Conduct. La version la plus récente du Code of Conduct peut être consultée, à tout moment, sur l'intranet de Gimv ou le site web de Gimv.

2.2 GIMV COMPLIANCE & ESG OFFICE

Le Gimv Compliance & ESG Office, qui est aujourd'hui constitué des personnes mentionnées ci-après, a été désigné par le Conseil d'Administration de la Société pour contrôler la conformité au présent Code of Conduct et pour traiter les matières stipulées aux présentes.

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

Si vous avez des questions ou des doutes sur la manière de se conformer à ce Code, veuillez contacter le Gimv Compliance & ESG Office par e-mail, à l'adresse compliance@gimv.com.

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

2.3 VIOLATIONS DU CODE OF CONDUCT

Aucune violation du Code of Conduct et ces annexes ne sera tolérée. Telles violations peuvent conduire à des actions disciplinaires conformes aux lois (y compris, mais non exclusivement, le droit pénal, de travail et des sociétés) et réglementations applicables.

Dans le cas où un Destinataire a une préoccupation de conformité (c.-à-d. a connaissance de tout comportement, qui est ou pourrait être incompatible avec le Code of Conduct et ses annexes et qui pourra ou pourrait avoir un impact sur l'intégrité de Gimv en tant qu'organisation), Gimv encourage tel Destinataire à le signaler. Il / elle peut le signaler au Gimv Compliance & ESG Office (compliance@gimv.com), conformément au Gimv Whistleblowing Policy (Annexe 2 ci-jointe).

Gimv ne toléra (i) aucune forme de représailles (directes ou indirectes) contre un Destinataire qui, de bonne foi, demande conseil, soulève une inquiétude ou signale un manquement ni (ii) aucune abuse des canaux de signalement de Gimv. Des mesures disciplinaires peuvent être prises dans de tels cas.

2.4 CONSULTATION, RECONNAISSANCE ET MISES A JOUR

Le Code of Conduct est accessible en permanence aux Employés sur l'intranet de Gimv et aux Administrateurs sur le site web de Gimv. Chaque Employé reçoit une copie du Code of Conduct au moment de sa publication et les Employés qui entrent en fonction après la Date de Publication en reçoivent une copie à la date de leur entrée en fonction au sein de Gimv ou peu après. Les Administrateurs reçoivent une copie du Code of Conduct à la date de leur nomination ou peu après.

Tous les Destinataires reconnaissent avoir pris connaissance du Code of Conduct et ces annexes, être liés par ledit Code et s'engagent à le respecter, en gage de quoi ils signent une déclaration établie sur le formulaire joint à l'Annexe 1.

2.5 DEFINITIONS

Les définitions suivantes s'appliquent, sauf si le contexte exige une interprétation différente :

Actions désignent toute action et titre de créance, ainsi que tout instrument dérivé et autres instruments financiers, dans le sens le plus large, liés aux présentes.

Administrateur a le sens qui lui est donné dans la section 2.1.

Code of Conduct a le sens qui lui est donné dans la section 2.1.

Date d'émission désigne la date à laquelle la version actuelle du Code of Conduct a été formellement approuvé par le Conseil d'Administration de Gimv pour la première fois et depuis laquelle ledit Code est devenu applicable à tous les Destinataires.

Date de mise à jour la plus récente désigne la date la plus récente à laquelle le Code of Conduct a été modifié après approbation par le Conseil d'Administration de Gimv.

Destinataire a le sens qui lui est donné dans la section 2.1.

Employé(e) a le sens qui lui est donné dans la section 2.1.

Gimv Compliance & ESG Office a le sens qui lui est donné dans la section 2.1.

Gimv Non-Trading List désigne la liste des Sociétés en Portefeuille cotées en Bourse dont les Actions ne peuvent être négociées par les Destinataires et leurs PEL. Cette liste est conservée

et tenue à jour par le Gimv Compliance & ESG Office et est accessible à tous les Destinataires sur l'intranet de Gimv.

Personne Étroitement Liée ou ***PEL*** désigne, par rapport à un Destinataire :

i. un(e) conjoint(e) ou un(e) partenaire qui est légalement considéré(e) comme équivalent(e) à un(e) conjoint(e) ;
ii. un enfant dont le Destinataire est responsable sur le plan juridique (cela inclut les enfants adoptés) ;
iii. un parent qui a fait partie du même ménage que le Destinataire pendant au moins un an à la date de la Négociation pertinente ; ou
iv. une personne morale, une fiducie ou un partenariat dont les responsabilités de gestion sont assurées par le Destinataire ou par une personne mentionnée au point (i), (ii) ou (iii), qui est directement ou indirectement contrôlé par le Destinataire ou cette personne, qui est constitué au profit du Destinataire ou de cette personne, ou dont les intérêts économiques sont essentiellement équivalents à ceux du Destinataire ou de cette personne.

Société en Portefeuille désigne toute entité dans laquelle le Groupe Gimv détient un investissement (au moyen d'Actions ou d'une autre manière) dans le cadre de ses activités professionnelles journalières.

Transaction doit être interprétée comme englobant toute transaction, dans son sens le plus large, portant sur des Actions.

3 INTERACTIONS AVEC LES SOCIETES EN PORTEFEUILLE

3.1 SOCIETES EN PORTEFEUILLE COTEES EN BOURSE

Les Employés, les Administrateurs et leurs Personnes Étroitement Liées (PEL) sont uniquement autorisés à effectuer des Négociations d'Actions émises par des Sociétés en Portefeuille cotées en Bourse si ces Négociations sont autorisées par le code de négociation de la Société en Portefeuille cotée en Bourse concernée et à condition que cette Société en Portefeuille cotée en Bourse ne figure pas dans le Gimv Non-Trading List. Le Conseil d'Administration peut permettre, dans des circonstances exceptionnelles, une Négociation d'Actions émises par des Sociétés en Portefeuille cotées en Bourse, figurant dans Gimv Non-Trading List (par exemple, en cas d'héritage).

3.2 SOCIETES EN PORTEFEUILLE NON COTEES EN BOURSE

Il est explicitement interdit qu'un Employé ou un Administrateur détienne, directement ou indirectement, des Actions de sociétés en portefeuille non cotées en Bourse. Les Employés et les Administrateurs prendront les précautions requises et raisonnables nécessaires pour empêcher que ces participations soient détenues par leurs PEL respectives. Cette interdiction générale est applicable sauf dans le cas d'une exemption explicite et écrite pouvant être autorisée par le Conseil d'Administration et soumise aux conditions de cette autorisation.

3.3 REMUNERATIONS POUR LES MISSIONS DANS DES SOCIETES EN PORTEFEUILLE

Pour éviter toute ambiguïté, cette section 3.3 ne s'applique à aucun Administrateur qui occupe un poste de membre ou d'observateur d'un conseil d'administration, d'un conseil de surveillance ou d'un conseil consultatif (liste non exhaustive de postes et des organes de l'entreprise) d'une Société en Portefeuille cotée en Bourse de Gimv.

Toutes les rémunérations, de quelque type, revenant de droit aux Employés en vertu d'un poste de membre ou d'observateur d'un conseil d'administration, d'un conseil de surveillance ou d'un conseil consultatif (liste non exhaustive de postes et des organes de l'entreprise) d'une Société en Portefeuille de Gimv, doivent être payées à Gimv (ou l'entité du Groupe Gimv désignée aux présentes), de préférence directement par cette Société en Portefeuille à Gimv. Au cas où cette rémunération aurait été payée à un Employé, l'Employé transférera immédiatement cette rémunération vers un des comptes bancaires de Gimv, indiqués sur le papier à en-tête de Gimv.

La rémunération, au sens de cet article, englobe (de manière non exhaustive), la rémunération variable des administrateurs, les jetons de présence, les honoraires, les frais de gestion, les services ou les frais de consultation et toutes les autres formes similaires de rémunération.

4 ETHIQUE DES AFFAIRES ET INTEGRITE

L'ambition de Gimv est de construire et de développer des sociétés performantes actif dans des marchés de croissance attractifs en créant de la valeur en termes de stratégie et de business model, d'expansion internationale et d'excellence opérationnelle. Dans ce contexte, Gimv a traduit sa vision de l'avenir durable de l'économie et de la société en cinq plateformes d'investissement : Consumer, Healthcare, Life Sciences, Smart Industries et Sustainable Cities.

En réalisant son ambition, Gimv attend de ses Sociétés en Portefeuille et de leurs administrateurs, dirigeants, cadres, employés et autres représentants qu'ils maintiennent des normes éthiques élevées, adoptent constamment un comportement exemplaire et recherchent l'excellence. C'est pourquoi Gimv et ses Employés et Administrateurs sont tenus de fixer la norme en matière de respect, d'éthique des affaires et d'intégrité.

De plus, Gimv s'engage à ne travailler qu'avec des tiers (y compris des intermédiaires et des conseillers) dont la conduite est conforme aux normes et aux principes énoncés ci-dessous.

4.1 DES INVESTISSEMENTS RESPONSABLES

Gimv est une société de capital-investissement européenne leader, responsable et sociétale-consciencieuse. Par conséquent, Gimv s'engage à ne pas s'investir et à veiller à ce que ses Sociétés en Portefeuille n'investissent pas dans des sociétés ou des entreprises suivantes :

- dont les activités, produits ou services sont réputés illégaux en vertu de toute loi, réglementation ou convention internationale applicable dans la juridiction concernée (notamment l'esclavage, l'exploitation, le travail forcé, la traite des êtres humains, le travail des enfants, la prostitution, du crime organisé);
- qui sont impliqués dans la production, la vente, l'utilisation ou le commerce d'armes, d'armes de destruction massive ou d'armes inhumaines ou de composants critiques associés (y compris mais non limité aux armes nucléaires, chimiques et radiologiques, aux mines terrestres et aux bombes). Des biens, services ou technologies intelligentes et solutions défensives ou non-offensives dans des domaines tels que l'avionique, le radar, le sonar, l'instrumentation, la communication et la protection (non exhaustive) peuvent être conformes à la politique d'investissement responsable de Gimv après une évaluation appropriée par le Gimv Compliance & ESG Office;
- dont les activités contribuent directement ou indirectement au financement du terrorisme ;
- qui sont actifs ou impliqués dans le développement, l'exploitation, la vente, la distribution, la gestion ou la commerce de produits et/ou de services et/ou d'installations qui, directement ou indirectement, sont liés au jeu, au tabac ou à la pornographie.

En cas de doute sur le fait que les activités d'une Société en Portefeuille (potentielle) puissent répondre aux critères susmentionnés, veuillez contacter le Gimv Compliance & ESG Office.

Gimv attend de ses Sociétés en Portefeuille qu'elles soient un partenaire engagé, constructif et digne de confiance qui s'engage à :

- se conformer aux lois, règlements ou conventions internationales applicables ;
- respecter le droit de la concurrence dans ses relations avec les concurrents, les fournisseurs et les clients ;
- ne jamais participer à des pots-de-vin, corruption ou comportement similaire ;
- respecter des normes élevées d'intégrité commerciale et se comporter de manière éthique, y compris, mais sans s'y limiter :
    - avoir une approche responsable et durable de la gestion environnementale de son entreprise
    - respecter les droits de ses employés, les traiter équitablement et préserver un milieu de travail sain et sécuritaire
    - installer une culture de gouvernance appropriée, de gestion des risques et de la conformité

4.2 ENVIRONNEMENT DE TRAVAIL

Tous les Destinataires doivent respecter les différences individuelles de chaque personne active au sein de Gimv, comme Employé ou Administrateur. Tous les Destinataires doivent donc se respecter mutuellement et réaliser les objectifs de Gimv ensemble sans distinction de race, d'ethnicité, de religion, d'origine nationale, de genre, d'orientation sexuelle, de handicap, d'âge, de situation de famille ou de toute autre référence. Aucune forme de discrimination illicite ou du comportement (sexuel) inapproprié / inacceptable ne sera tolérée.

Gimv accorde une grande valeur à l'établissement et au maintien d'un environnement de travail où les personnes sont traitées avec dignité et respect, et qui est caractérisé par la confiance mutuelle et l'absence de toute forme (directe ou indirecte) d'intimidation, d'oppression et d'exploitation.

4.3 INFORMATIONS CONFIDENTIELLES

Tous les Destinataires ont ou peuvent avoir accès à des informations confidentielles portant sur (i) Gimv, (ii) les activités commerciales de Gimv en tant que société à capital privé effectuant des investissements dans des Sociétés en Portefeuille, et (iii) les Sociétés en Portefeuille (potentielles) de Gimv et de tierces parties. Par conséquent, tous les Destinataires doivent prendre les précautions nécessaires pour conserver le caractère confidentiel de ces informations et prévenir toute communication illicite à des concurrents ou à d'autres tierces parties non autorisées.

Pour protéger l'intégrité et la sécurité de ses propres données, Gimv a mis en place le Gimv Data Protection Framework conçu pour détecter et alerter les violations de données illégales ou les pertes de l'intérieur de l'organisation. Une description détaillée du fonctionnement du Gimv Data Protection Framework (y compris la manière dont Gimv traite tout impact possible sur la vie privée des employés) est ajoutée au Code of Conduct en tant qu'annexe 3.

4.4 CONFLITS D'INTERETS

Des conflits d'intérêts peuvent surgir en cas d'intérêt personnel direct ou indirect dans une décision prise par et pour Gimv. En cas de conflit d'intérêts, l'impartialité des décisions n'est jamais garantie.

En conséquence, outre les règles du Code belge des Sociétés applicables aux conflits d'intérêts des Administrateurs ou des membres des comités de direction, tous les Destinataires feront preuve d'un jugement équitable, objectif et impartial dans toutes les négociations commerciales de Gimv, en plaçant toujours les intérêts de Gimv au-dessus de tout intérêt personnel en ce qui concerne les matières commerciales de Gimv.

Aucun Destinataire n'utilisera sa position pour obtenir tout bénéfice direct ou indirect et tout Destinataire communiquera au Gimv Compliance & ESG Office tout conflit d'intérêts, toute relation qu'il a avec une Société en Portefeuille (potentielle) autre que la relation découlant du contexte des activités journalières de Gimv, d'un fournisseur ou d'un consultant tiers travaillant pour Gimv ou un concurrent de Gimv. Le Gimv Compliance & ESG Office se réserve le droit d'informer le Conseil d'Administration de Gimv de ce conflit d'intérêts communiqué. Tous les destinataires doivent s'abstenir de participer à toute transaction ou activité commerciale susceptible d'être considérée comme ou de donner lieu à un conflit d'intérêts.

Si un Destinataire n'est pas sûr si une situation donnée représente ou non un conflit d'intérêts, il est invité à demander conseil au Gimv Compliance & ESG Office.

4.5 UTILISATION DES RESSOURCES DE GIMV

Les Destinataires ne sont pas autorisés à utiliser un(e) quelconque ressource, actif ou solvabilité de Gimv (ou de toute autre entité de Groupe Gimv) ou d'une Société en Portefeuille en vue de réaliser des bénéfices en dehors de l'exercice normal des activités de Gimv ou à des fins illégales. Gimv comprend que les Employés doivent, le cas échéant, traiter pendant leur temps de travail des affaires personnelles qui ne peuvent pas être gérées en dehors des heures normales de travail, mais cette utilisation du temps de travail ne peut être excessive. En cas de doute, l'Employé est encouragé à demander l'approbation du chef de département correspondant.

Pour des directives concernant l'utilisation correcte des installations et environnement IT de Gimv, nous nous référons à une IT Policy distincte qui est ajouté au Code of Conduct en tant qu'annexe 5 et peut également être consultée sur l'intranet de Gimv.

4.6 CONCURRENCE LOYALE

Gimv accorde une grande valeur à la concurrence loyale et souhaite mener ses activités commerciales de manière éthique et intègre. Donc, Gimv ne fait et ne fera jamais des investissements ou ne conclut et ne conclura jamais des accords commerciaux qui faussent, éliminent ou découragent la concurrence ou qui fournissent des avantages concurrentiels illégitimes.

4.7 CADEAUX ET POTS-DE-VIN

Gimv est une société commercialement active et, en tant que telle, elle se comporte avec ses Sociétés en Portefeuille, consultants, fournisseurs de services et toutes les autres parties selon les pratiques commerciales raisonnables et communes. Par conséquent, le fait d'offrir ou d'accepter par des Destinataires des cadeaux ou des faveurs quotidiens, ainsi que des repas occasionnels, est considéré comme relevant de pratiques commerciales raisonnables et

communes s'ils sont modestes (en valeur et en fréquence) et appropriés (en temps et en lieu). L'échange d'espèces ou d'équivalents d'espèces n'est en aucun cas acceptable.

Gimv interdit formellement, sous toutes ses formes, la distribution, l'offre ou l'acceptation de cadeaux et de pots-de-vin devant servir à obtenir ou à conserver des marchés ou d'autres avantages ou promesses illégitimes. Enfin, le fait de déguiser des cadeaux ou des divertissements en dons de bienfaisance, est considéré comme une violation du Code of Conduct.

Lorsqu'un Destinataire n'est pas sûr si une situation donnée relève ou non de pratiques commerciales raisonnables et communes, il est invité à demander conseil au Gimv Compliance & ESG Office.

Gimv peut prendre des mesures (y compris entamer une procédure judiciaire) à tout moment contre des Employés, Administrateurs, sociétés en portefeuille (potentielles), consultants ou fournisseurs de services (liste non exhaustive) qui se rendent coupables ou sont coupables de (participer à) les pots-de-vin, la fraude, la fixation des prix, les services de facturation qu'ils n'ont pas fournis ou la corruption.

5 COMMUNICATION EXTERNE ET MEDIAS SOCIAUX

Le Président, le CEO, les autres membres du Comité Exécutif et toute autre personne spécifiquement désignée à cet effet sont les seules personnes responsables de la communication externe de Gimv et du maintien des contacts avec les médias. Ainsi, toutes les questions provenant des médias (quelle que soit la forme) doivent être immédiatement transmises à une ou toutes les personnes précitées.

Tous les Destinataires doivent contribuer à la protection et à l'amélioration de l'image de Gimv. Par conséquent, tous les Destinataires doivent être conscients de ce qu'ils écrivent au sujet de Gimv sur des sites web, des blogs ou des réseaux sociaux, y compris, mais sans aucune limitation, sur Facebook, Twitter et LinkedIn. Gimv a mis certaines directives internes sur les réseaux sociaux à la disposition des Destinataires sur l'Intranet de Gimv.

6 REGLES ET REGLEMENTATIONS

Faire des affaires conformément aux normes éthiques les plus élevées entraîne évidemment le respect de la primauté du droit et le respect de la législation en vigueur. Toute violation de la loi ou des réglementations peut entraîner des sanctions de nature civile, administrative ou criminelle imposée à Gimv et au Destinataire individuel impliqué. Cela peut avoir des conséquences négatives pour la carrière du Destinataire particulier impliqué. Pour toute question sur la législation en vigueur, veuillez consulter le département juridique ou le Gimv Compliance & ESG Office.

ANNEXE 1
FORMULAIRE DE RECONNAISSANCE

À l'attention de : Gimv NV

Karel Oomsstraat 37

2018 Anvers

Belgique

(ci-après la ***Société***)

J'accuse réception par la présente du Code of Conduct de Gimv y compris ses annexes (comme le Gimv Whistleblowing Policy, le Gimv Data Protection Framework, Le Gimv Expense Policy et le Gimv IT-Policy) qui m'a été fourni avec cette reconnaissance.

Je confirme avoir lu et compris le Code of Conduct, avec ses modifications successives, et j'accepte de le respecter.

Signature :……..

Date :……

Veuillez remplir ce formulaire et le retourner au Gimv Compliance & ESG Office par e-mail à l'adresse compliance@gimv.com.

ANNEXE 2
GIMV WHISTLEBLOWING POLICY

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

WHISTLEBLOWING POLICY

(POLITIQUE DE DÉNONCIATION)

TABLE DES MATIÈRES

CONTEXTE

Gimv NV est une société à responsabilité limitée de droit belge dont le siège social est situé Karel Oomsstraat 37, 2018 Antwerpen, Belgique et enregistrée auprès de la Banque-Carrefour des Entreprises sous le numéro 0220.324.117 (ci-après "**Gimv**" ou la "**Société**").

Gimv s'engage à respecter les normes les plus élevées en matière d'ouverture, d'intégrité, de transparence et de responsabilité. Un aspect important de ces valeurs est de fournir à tous les actionnaires, membres de la direction, membres permanents, temporaires et anciens membres du personnel, agents, sous-traitants et autres affiliés[1] (ci-après dénommés individuellement "**Destinataire**" et collectivement "**Destinataires**") de Gimv et de ses filiales (ci-après **"Groupe Gimv"**) un processus efficace pour faire part de leurs Inquiétudes concernant l'une des questions énumérées dans la présente politique et procédure de dénonciation (la "**Politique de Dénonciation"**). Pour éviter tout doute, les filiales n'incluent pas les sociétés de portefeuille externes du groupe Gimv et TDP ni les fonds gérés par TDP, TINC.

La "**Dénonciation"** est le processus par lequel une personne fait part de ses inquiétudes de bonne foi sur des questions qui semblent soulever de sérieuses Inquiétudes au sein de Gimv.

Gimv reconnaît la valeur du signalement par les Destinataires d'Inquiétudes concernant ses activités et ses opérations (dans un tel cas, le Destinataire est qualifié de **"Dénonciateur"**).

Gimv encourage donc les Destinataires à exprimer de telles Inquiétudes en interne en déposant un rapport le cas échéant (un tel rapport étant un "**Rapport de Dénonciation"**).

Conformément à son propre engagement, Gimv espère que tous les Destinataires percevront le fait de s'exprimer comme une contribution positive à la protection et à l'amélioration de la culture de travail, de la réputation et du succès de Gimv. Tous les Destinataires ont la responsabilité de signaler rapidement toute activité suspecte, conformément à la présente Politique de Dénonciation.

L'objectif de la présente Politique de Dénonciation est donc de fournir un cadre et un processus permettant aux Destinataires de "dénoncer" en interne les violations de la loi, de la réglementation, de la conformité ou de l'éthique. Elle définit le processus par lequel ces Inquiétudes peuvent être exprimées et faire l'objet d'une action. Il précise également quand et comment la protection contre les représailles s'applique, ainsi que la manière dont la confidentialité, les conflits d'intérêts et les privilèges juridiques (le cas échéant) doivent être gérés.

Les objectifs de cette Politique de Dénonciation sont de garantir que :

- Les Destinataires savent clairement quand et comment s'exprimer et déposer un Rapport de Dénonciation ;
- Les Destinataires ont une compréhension claire des fonctions internes et des mesures mises en œuvre pour garantir l'indépendance et l'efficacité de la procédure d'alerte ;
- Gimv est en mesure de donner suite aux Inquiétudes signalées de manière efficace et opportune.

[1] Cela inclut tous les travailleurs dans un contexte professionnel, les membres actuels et anciens ainsi que les personnes engagées dans un processus de recrutement, c'est-à-dire les employés, les travailleurs indépendants, les bénévoles, les stagiaires (non rémunérés), les actionnaires, les membres des organes de gestion, d'administration ou de surveillance de Gimv.

PARTIE 1. INQUIÉTUDES À SIGNALER

Gimv encourage tous les Destinataires à déposer un Rapport de Dénonciation lorsqu'ils ont une **croyance raisonnable et légitime** que l'une des violations suivantes est, a été ou est susceptible d'être commise en relation avec :

- Les marchés publics ;
- Services, produits et marchés financiers, et prévention du blanchiment de capitaux et du financement du terrorisme ;
- Sécurité et conformité des produits ;
- Sécurité des transports ;
- Protection de l'environnement ;
- Radioprotection et sûreté nucléaire ;
- Sécurité des aliments destinés à l'alimentation humaine et animale, santé et bien-être des animaux ;
- La santé publique ;
- Protection des consommateurs ;
- Protection de la vie privée et des données à caractère personnel, et sécurité des réseaux et des systèmes d'information ;
- Non-respect des lois antitrust ou de la concurrence ;
- Une violation portant atteinte aux intérêts financiers de l'Union européenne[2] ;
- Une violation des politiques et procédures de Gimv[3] ;

(une telle situation est définie ci-après comme une "**Inquiétude à Signaler"**).

La présente Politique de Dénonciation **ne** couvre **pas** les griefs spécifiques aux conditions de travail, y compris, mais sans s'y limiter, les plaintes sociales, de travail et d'emploi, qui doivent être traitées conformément aux procédures RH applicables, et, un Rapport de Dénonciation ne doit pas être déposé concernant ces griefs spécifiques,

Les Destinataires n'ont pas la responsabilité d'enquêter sur l'affaire qu'ils ont (l'intention de) signaler. Il incombe à Gimv de veiller à ce qu'une enquête soit menée après réception du Rapport de Dénonciation.

PARTIE 2. PRINCIPES

Les Destinataires doivent toujours agir conformément aux principes généraux suivants :

- Les Inquiétudes à Signaler doivent toujours être signalées de bonne foi, cette dernière étant présumée ;
- Les Inquiétudes à Signaler peuvent être signalées même sans preuve à l'appui : il suffit de croire qu'une Inquiétude à Signaler a lieu ou est sur le point d'avoir lieu ;
- Seules les Inquiétudes directes à Signaler doivent être signalées et aucune déclaration "par ouï-dire" ne doit être faite ;
- Le signalement des Inquiétudes ne doit pas servir des objectifs vindicatifs ou personnels (ce qui pourrait être qualifié de signalement de mauvaise foi) ;
- Les Inquiétudes à Signaler peuvent être signalés de manière nominative ou anonyme ;

[2] liés à la lutte contre la fraude, la corruption et toute autre activité illégale affectant les dépenses de l'Union Européenne, la perception des recettes et des fonds de l'Union ou les actifs de l'Union Européenne.
[3] Les politiques et procédures de Gimv sont établies non seulement pour se conformer aux obligations légales et spécifiques, mais aussi pour refléter les orientations appropriées et favoriser les bonnes pratiques et la culture qui soutiennent le succès de Gimv.

- Les droits et protections établis dans la présente Politique de Dénonciation ne peuvent être abandonnés par aucun accord, politique, formulaire ou condition d'emploi.

PARTIE 3. PROTECTION DES DÉNONCIATEURS

1. Protection des Rapports *de bonne foi*

Gimv protégera tout Destinataire ayant déposé un Rapport de Dénonciation de *bonne foi*, même s'il s'avère être dans l'erreur, contre le licenciement et toute autre forme de représailles, de menace ou d'action hostile.

Les mesures de rétorsion interdites comprennent, sans s'y limiter, la suspension, la mise à pied, le licenciement ou des mesures équivalentes, la rétrogradation ou le refus de promotion, le transfert de fonctions, le changement de lieu de travail, la réduction des salaires, le refus de formation, la discrimination, la coercition, l'intimidation, le harcèlement, etc.

Toute forme de représailles de ce type peut entraîner des mesures disciplinaires conformément aux règles et politiques applicables de Gimv, pouvant aller jusqu'au licenciement, ainsi que la saisine des autorités judiciaires.

Cette protection est également accordée aux lanceurs d'alerte qui transmettent des informations qu'ils ont obtenues en dehors d'un contexte professionnel.

Cette protection est également accordée, le cas échéant, aux facilitateurs, collègues ou parents du Dénonciateur qui sont également en relation professionnelle avec l'employeur ou le client ou le bénéficiaire de services du Dénonciateur, ainsi qu'à toute entité juridique que le Dénonciateur possède, pour laquelle il travaille ou avec laquelle il est autrement en relation dans un contexte professionnel.

Les Dénonciateurs n'encourent aucune responsabilité pour avoir obtenu ou obtenu l'accès à des Inquiétudes à Signaler, à condition que l'obtention ou l'accès à ces informations ne constitue pas une infraction pénale distincte.

2. Pas de protection en cas de déclaration *de mauvaise foi*

Gimv prend très au sérieux tout dépôt d'un Rapport *dont on sait qu'il est faux* ou qui est fait *de mauvaise foi*, par malveillance, par imprudence ou dans un but de gain personnel.

Si l'enquête conclut qu'un Destinataire a déposé un Rapport de Dénonciation de mauvaise foi, Gimv peut prendre des mesures disciplinaires à l'encontre du Dénonciateur conformément à ses règles et politiques applicables, pouvant aller jusqu'au licenciement, ainsi que la saisine des autorités judiciaires.

PARTIE 4. CONFIDENTIALITÉ

Les Rapports de Dénonciation peuvent être déposés de manière nominative ou anonyme.

Cette Politique de Dénonciation garantit que tous les Rapports de Dénonciation seront traités rapidement, de manière indépendante et approfondie, sans porter préjudice aux Destinataires, à leur carrière ou à leur réputation. Gimv protégera dans tous les cas la confidentialité et l'identité des Dénonciateurs et des autres parties impliquées dans le rapport et l'enquête interne qui s'ensuit, le cas échéant. La personne responsable du traitement du Rapport de Dénonciation agira en tant que responsable de la protection de l'identité.

Une discrétion totale est attendue de la part de toutes les parties impliquées dans l'enquête et les procédures qui en découlent.

Cette Politique de Dénonciation empêche également le personnel non autorisé d'accéder aux informations signalées.

L'identité du Dénonciateur et des autres personnes concernées ne peut être levée que dans l'un des cas exhaustifs suivants :

- Avec le consentement exprès des personnes dont l'identité est protégée, sachant que le Dénonciateur peut s'identifier à tout moment ;
- À la demande des autorités judiciaires ou réglementaires compétentes, dans la mesure où Gimv est légalement tenue de coopérer avec ces organes ;
- Si l'Inquiétude à Signaler est utilisée dans le cadre d'une procédure judiciaire ;
- Lorsque vous demandez conseil à un comptable ou à un avocat ;
- Lorsque l'information est déjà dans le domaine public,

en gardant à l'esprit que l'objectif premier de cette Politique de Dénonciation est de protéger les Dénonciateurs de bonne foi contre des mesures disciplinaires, des actions de représailles ou une atteinte à la réputation ou à la confiance.

PARTIE 5. REPORTING INTERNE

Les canaux de compte rendu internes doivent être préférés au compte rendu externe qui est soumis à des conditions spécifiques (voir **PARTIE 6.** ci-après).

1. Responsable de la Dénonciation

Gimv a confié la responsabilité interne du traitement (c'est-à-dire la réception et le suivi) des Rapports de Dénonciation, y compris la conduite d'enquêtes et la recommandation d'actions ultérieures, le cas échéant, au Gimv Compliance & ESG Office. Parmi les membres du Gimv Compliance & ESG Office, le Compliance Manager de Gimv est désigné comme le **"Responsable de la Dénonciation"**.

La nomination d'un Responsable de la Dénonciation garantit le traitement de la question conformément aux principes de gouvernance que sont la compétence, la diligence, l'équité et l'impartialité.

2. Dépôt d'un Rapport de Dénonciation

Les Rapports de Dénonciation doivent être déposés auprès du Responsable de la Dénonciation, par courrier électronique, conformément aux directives fournies aux Dénonciateurs à l'**ANNEXE 1**.

Par exception, lorsqu'il n'est pas approprié pour le Responsable de la Dénonciation de mener l'enquête (par exemple en raison d'un conflit d'intérêts, y compris lorsque le Responsable de la Dénonciation est le sujet du rapport), le Rapport de Dénonciation peut être déposé auprès de l'un des autres membres du Compliance & ESG Office de Gimv, notamment le CEO, le CFO et le CLO - Secrétaire général ou le président du conseil d'administration de Gimv.

3. Accusé de réception

Le Responsable de la Dénonciation doit accuser réception du rapport au Dénonciateur dans les sept (7) jours ouvrables suivant son dépôt (sauf si le rapport a été déposé de manière anonyme).

Le Responsable de la Dénonciation indique à cette occasion, le cas échéant et dans la mesure du possible, si le Rapport de Dénonciation entre dans le champ d'application de la Politique de Dénonciation et est donc considéré comme recevable, y compris les droits et obligations attachés à ce signalement et les mesures ultérieures à prendre. Il précise également qu'une réunion peut être organisée à la demande du Dénonciateur.

4. Recevabilité

Dès réception d'une Dénonciation, le Responsable de la Dénonciation vérifie la recevabilité de la Dénonciation, qui est soumise aux conditions cumulatives suivantes :

- Les faits signalés entrent dans le cadre de la Politique de Dénonciation, c'est-à-dire qu'ils constituent une Inquiétude à Signaler ;
- La personne concernée entre dans le champ d'application de la Politique de Dénonciation, c'est-à-dire qu'elle remplit les conditions requises pour être un Dénonciateur ; et
- Les conditions formelles d'un Rapport de Dénonciation ont été remplies.

5. Évaluation préliminaire du Rapport de Dénonciation.

Dans la mesure du possible, le Responsable de la Dénonciation procède à une évaluation primaire des informations fournies dans le Rapport de Dénonciation afin d'en déterminer l'importance, notamment :

- Les règles, obligations, conduites ou normes qui auraient été violées ;
- Les faits sous-jacents menant au rapport ;
- Le nom, la position et la fonction des personnes présumées responsables de l'Inquiétude à Signaler ;
- Le nom, le poste et la fonction du Dénonciateur (le cas échéant) et de toute autre personne impliquée.

Pour se conformer à cette obligation, le Responsable de la Dénonciation remplira un formulaire de suivi du Rapport de Dénonciation.

6. Enquête interne

Le Responsable de la Dénonciation doit agir en temps utile, avec la diligence requise et prendre toutes les mesures disponibles pour mener une enquête interne et remédier à la violation signalée (le cas échéant), que le Rapport de Dénonciation soit déposé nominativement ou anonymement.

Le Responsable de la Dénonciation peut interagir à tout moment avec le Dénonciateur, le cas échéant, pour procéder à cette évaluation.

Le Responsable de la Dénonciation doit, dans tous les cas, fournir un suivi et un retour d'information au Dénonciateur sur les actions ou l'absence d'actions dans un délai raisonnable, étant donné la nécessité de traiter rapidement l'Inquiétude qui fait l'objet de la dénonciation.

Ce délai ne devrait pas dépasser trois (3) mois mais pourrait être étendu à six (6) mois si nécessaire en raison des circonstances spécifiques de l'affaire, notamment la nature et la complexité de l'objet du Rapport de Dénonciation, qui peuvent nécessiter une longue enquête.

PARTIE 6. REPORTING EXTERNE

1. Rapport à l'autorité compétente

Le Dénonciateur peut partager une Inquiétude à Signaler auprès d'un organisme de réglementation ou d'une autorité externe compétents, y compris les autorités pénales, **à condition que** :

- *Après le rapport interne* : ils ne soient pas satisfaits du résultat du processus interne - y compris s'il n'y a pas eu de suivi du rapport interne dans le délai spécifié ci-après ; *ou*
- *Directement, c'est-à-dire sans rapport interne* : s'il craint que son Inquiétude ne soit pas traitée de manière appropriée, indépendante et objective en interne. Le Dénonciateur doit toutefois examiner attentivement la situation avant de décider de déposer directement un rapport externe, car le rapport interne doit toujours être préféré.

2. Divulgation publique

Les Dénonciateurs ont le droit de faire une divulgation publique[4] et de bénéficier des droits et des protections prévus par la procédure, **à condition que** :

- Le Dénonciateur ait d'abord signalé l'affaire à la fois en interne et en externe, ou en externe à l'organisme de réglementation ou à l'autorité compétents, mais aucune mesure appropriée n'a été prise en réponse à ce signalement dans le délai spécifié ci-dessus **(PARTIE 5**, **Section 3)**; ou
- Le Dénonciateur a des motifs raisonnables de croire que :
  - La violation peut constituer un danger imminent ou manifeste pour l'intérêt public, par exemple en cas d'urgence ou de risque de dommages irréversibles ; ou
  - Dans le cas d'un compte rendu externe, il existe un risque de représailles ou il y a peu de chances que la violation soit effectivement traitée, en raison des circonstances particulières de l'affaire, comme celles où les preuves peuvent être dissimulées ou détruites ou celles où une autorité peut être de connivence avec l'auteur de la violation ou impliquée dans la violation.

Le Dénonciateur ne doit utiliser la voie de la divulgation publique qu'en **dernier recours, et seulement si les** conditions ci-dessus sont remplies.

Les Dénonciateurs sont conscients qu'ils peuvent **perdre les** droits et protections garantis dans cette procédure en cas d'utilisation abusive du canal de signalement public[5] .

[4] C'est-à-dire par le biais des réseaux sociaux, de communiqués de presse, d'interviews publiques ou de tout autre canal ayant un effet similaire.
[5] Les dénonciateurs qui utilisent les canaux de communication publique conformément à la présente procédure et politique ne seront pas considérés comme ayant enfreint une quelconque restriction à la divulgation d'informations et n'encourront aucune responsabilité de quelque nature que ce soit en ce qui concerne cette divulgation publique.

PARTIE 7. FORMATION

Le Responsable de la Dénonciation est chargé de s'assurer que les Destinataires reçoivent une formation adéquate sur la présente Politique de Dénonciation, qu'ils comprennent et sont informés de leurs devoirs, de leurs droits et de leur protection, le cas échéant.

Les formations doivent être dispensées de manière continue, à la fois lors du recrutement de nouveaux employés et périodiquement si nécessaire.

Une fois tous les deux ans, le Responsable de la Dénonciation vérifie que tous les Destinataires ont été formés de manière adéquate à la présente Politique de Dénonciation.

Le Responsable de la Dénonciation fait des communications périodiques, le cas échéant, pour sensibiliser les Destinataires à la présente Politique de Dénonciation.

PARTIE 8. TENUE DES REGISTRES ET CONFIDENTIALITÉ DES DONNÉES

Gimv a mis en place un registre de dénonciation (le **Registre**) afin de conserver une trace de chaque rapport déposé en interne, qu'il soit recevable ou non. Ce Registre est géré sous le contrôle et la supervision du Responsable de la Dénonciation.

Le Registre enregistre :

- La date et l'heure du rapport ;
- La nature du rapport ;
- Les règles, obligations, conduites ou normes qui auraient été violées ;
- Un résumé des faits sous-jacents menant au rapport ;
- Le nom, le poste et la fonction des personnes responsables de la violation ;
- Le nom, le poste et la fonction du Dénonciateur (le cas échéant) ;
- La fonction et le poste des autres parties concernées ;
- Les mesures prises à la suite du dépôt du rapport (dans le cadre de la procédure d'enquête) ;
- La conclusion sur la véracité et la matérialité des faits et des Inquiétudes signalées ;
- Les mesures prises sur la base de la conclusion de la procédure d'enquête ;
- Tout autre élément pertinent.

Les dossiers doivent être conservés pendant cinq (5) ans après la résolution de l'affaire.

Gimv s'assure que toutes les données personnelles collectées à la suite de la présente Politique de Dénonciation, y compris dans le cadre de tout dépôt de rapport, enquête et procédure connexe, sont traitées dans le respect de la conformité de la loi et des obligations applicables en matière de confidentialité des données. Cela inclut le Règlement (UE) 2016/679 du 27 avril 2016 (le GDPR) *et* la loi Belge du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, ainsi que les politiques de confidentialité de Gimv**.**

Gimv veille également à fournir le plus haut niveau de sécurité en ce qui concerne la protection des données sensibles (le cas échéant).

PARTIE 9. SUIVI ET MISE EN ŒUVRE DE LA PROCÉDURE

1. Mise en œuvre

La présente Politique de Dénonciation a été approuvée par le Conseil d'Administration. Le Responsable de la Dénonciation a la responsabilité principale et quotidienne d'assurer la mise en œuvre effective de cette Politique de Dénonciation.

2. Surveillance

Le Responsable de la Dénonciation doit surveiller l'utilisation et l'efficacité de la Politique de Dénonciation de manière continue, la réviser et la mettre à jour le cas échéant. Toute amélioration

de la politique d'alerte identifiée doit être apportée dès que possible, mais au minimum une fois par an. Les commentaires, suggestions et questions concernant cette Politique de Dénonciation doivent être adressés au Responsable de la Dénonciation.

ANNEXE 1 : DIRECTIVES POUR LE PERSONNEL EN MATIÈRE DE DÉNONCIATION DES DYSFONCTIONNEMENTS

Si vous souhaitez faire part à Gimv d'une Inquiétude à Signaler, veuillez envoyer vos Rapports de Dénonciation par courrier électronique directement au Responsable de la Dénonciation à l'adresse suivante : compliance@gimv.com.

Veuillez inclure au moins les détails suivants dans votre courriel pour que votre Rapport de Dénonciation soit recevable :

- Les faits sous-jacents conduisant au rapport, y compris mais sans s'y limiter :
  - *Les faits/événements dont vous avez été témoin ou dont vous soupçonnez l'existence.*
  - *Les circonstances dans lesquelles les faits/événements ont eu lieu (cadre, contexte, dates...)*
  - *s'il s'agit d'une faute/violation permanente ou d'un événement ponctuel.*
- L'identité, les fonctions et les coordonnées des personnes faisant l'objet du signalement (c'est-à-dire l'auteur présumé du délit) ;
- En cas de déclaration nominative, votre identité, vos fonctions et vos coordonnées.

Veuillez également *joindre* à votre courriel tout document justifiant et/ou toute preuve de l'Inquiétude à Signaler.

Vous devez coopérer pleinement et fournir toutes les informations pertinentes demandées par Gimv à la suite du dépôt d'un Rapport de Dénonciation (si celui-ci est nominatif) ainsi que tout au long de l'enquête interne (le cas échéant).

Dans ce contexte, vous devez toujours respecter vos devoirs de confidentialité et de loyauté envers Gimv.

Vous avez le droit de déposer votre Rapport de Dénonciation de manière anonyme. Notez toutefois que, si vous décidez de rester anonyme :

- Vous ne recevrez pas d'accusé de réception ni de retour d'information sur votre Rapport de Dénonciation ;
- Le Responsable de la Dénonciation ne sera pas en mesure de vous contacter pour obtenir des informations supplémentaires ou des preuves à l'appui de votre rapport et de l'enquête (le cas échéant).

Veuillez donc vous assurer de fournir autant d'informations spécifiques et détaillées et de documents justificatifs que possible, afin de permettre au Responsable de la Dénonciation d'évaluer correctement la situation et de donner suite à votre Rapport de Dénonciation.

ANNEXE 3
GIMV DATA PROTECTION FRAMEWORK

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

GIMV DATA PROTECTION FRAMEWORK

Table of content

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

ANNEXE 4
GIMV EXPENSE POLICY

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

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.

ANNEXE 5
GIMV IT USER POLICY

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

GIMV IT USER POLICY

Table of content

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