Gimv

CODE OF CONDUCT

Datum van uitgifte:	20 september 2016
Datum van meest recente bijwerking:	16 mei 2023

1 INHOUDSOPGAVE

2 INLEIDING EN TOEPASSINGSGEBIED

2.1 TOEPASSINGSGEBIED

Deze ***Code of Conduct***, zoals goedgekeurd door de raad van bestuur van Gimv, is van toepassing op elke werknemer (met inbegrip van tijdelijke werknemers en stagiairs) van Gimv en haar dochterondernemingen (een ***Werknemer***), alsook elk lid van de raad van bestuur van Gimv (een ***Bestuurder***) (waarbij een Werknemer en een Bestuurder hierna samen een ***Geadresseerde*** worden genoemd). Voor alle duidelijkheid, de dochterondernemingen omvatten geenszins de externe portefeuilleondernemingen van Gimv noch de Gimv-Belfius infrastructuur joint venture TDP, TINC en de door TDP beheerde fondsen.

Deze Code of Conduct vormt een belangrijke algemene leidraad. Desalniettemin is dit geen uitputtend document dat anticipeert op elke situatie waarmee een Werknemer of een Bestuurder in zijn of haar dagelijkse activiteiten te maken kan krijgen. Gimv verwacht dat de Geadresseerden altijd handelen op een verantwoorde en plichtsbewuste manier. Ingeval een Geadresseerde vragen of twijfels heeft omtrent de bepalingen van de Code of Conduct of wil weten of een bepaalde handeling strijdig zou zijn met de bepalingen of de geest van de Code of Conduct, raadt Gimv die Geadresseerde aan om onmiddellijk contact op te nemen met de Gimv Compliance & ESG Office.

De Code of Conduct heeft betrekking op (i) interacties met portefeuilleondernemingen (die zowel Transacties in Effecten van Portefeuilleondernemingen omvatten als het innen van vergoedingen voor mandaten binnen Portefeuilleondernemingen), (ii) het bepalen van de norm voor een Werknemer of Bestuurder van Gimv inzake respect en integriteit en (iii) de communicatie naar het publiek. Sommige principes vervat in de Code of Conduct werden verder uitgewerkt in afzonderlijke policies en procedures. Zo werden de Gimv Whislteblowing Policy (klokkenluidersbeleid), het Gimv Data Protection Framework, de Gimv Expense Policy (onkostenbeleid) en de Gimv IT Policy toegevoegd als bijlagen bij deze Code of Conduct en worden geacht integraal deel uit te maken hiervan. Voor de toepasselijke interne regels inzake Transacties in Gimv-Effecten verwijzen we naar de afzonderlijke Dealing Code.

De Code of Conduct weerspiegelt een aantal basisbeginselen die Gimv hoog in het vaandel draagt, alsook beleidslijnen of procedures die de Geadresseerden moeten naleven. De Code of Conduct creëert echter geen enkel recht voor overheden, aandeelhouders, portefeuilleondernemingen, leveranciers, concurrenten of andere personen of entiteiten.

De Code of Conduct en haar bijlagen kunnen worden bijgewerkt en gewijzigd op grond van nieuwe wetten en regelgevingen of nieuwe belangrijke maatschappelijke ontwikkelingen. Alle Geadresseerden zullen per e-mail worden ingelicht over alle wijzigingen aan deze Code of Conduct. De laatste versie van de Code of Conduct kan te allen tijde geraadpleegd worden op het intranet of de website van Gimv.

2.2 GIMV COMPLIANCE & ESG OFFICE

De Gimv Compliance & ESG Office, dat vandaag is samengesteld uit de hierna vermelde personen, werd door de raad van bestuur van Gimv aangesteld om toe te zien op de naleving van deze Code of Conduct en om de hierin beschreven zaken te behandelen.

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

Bij vragen of twijfels over hoe u deze Code of Conduct dient na te leven, kunt u de Gimv Compliance & ESG Office mailen op het adres compliance@gimv.com.

2.3 SCHENDING VAN DE CODE OF CONDUCT

Schendingen van de Code of Conduct en haar bijlagen zullen niet worden getolereerd. Zulke schendingen kunnen leiden tot tuchtmaatregelen volgens de toepasselijke wetgeving (met inbegrip van maar niet beperkt tot het arbeidsrecht, strafrecht en vennootschapsrecht) en regelgevingen.

Ingeval een Geadresseerde een bezorgdheid heeft op vlak van compliance (bv. kennisneemt van een gedraging die mogelijk strijdig is met of ingaat tegen de Code of Conduct en haar bijlagen en die een impact zal of kan hebben op de integriteit van Gimv als organisatie), moedigt Gimv de Werknemer of Bestuurder aan om dit te melden. Hij/zij kan dit melden aan de Gimv Compliance & ESG Office (compliance@gimv.com) in lijn met de Gimv Whistleblowing Policy (klokkenluidersbeleid) (aangehecht als Bijlage 2).

Gimv tolereert (i) geen enkele vorm van (rechtstreekse of onrechtstreekse) vergelding tegen een Geadresseerde die ter goeder trouw advies vraagt, een kwestie naar voren brengt of wangedrag meldt, noch (ii) enig misbruik van de beschikbare Gimv meldingskanalen. In zulke gevallen kunnen tuchtmaatregelen worden opgelegd.

2.4 RAADPLEGING, INSTEMMING EN ACTUALISERING

De Code of Conduct kan steeds door de Werknemers worden geraadpleegd op het intranet van Gimv en door de Bestuurders op de website van Gimv. Elke Werknemer krijgt bij uitgifte een kopie van de Code of Conduct en Werknemers die beginnen te werken na de uitgiftedatum krijgen een kopie van de Code of Conduct op of kort na de datum waarop ze beginnen te werken bij Gimv. Bestuurders krijgen een kopie van de Code of Conduct op of kort na de datum van hun aanstelling.

Alle Geadresseerden bevestigen kennis te hebben genomen van en gebonden te zijn door de Code of Conduct en haar bijlagen en deze te zullen naleven, en ondertekenen hiertoe een verklaring die bijgevoegd is als bijlage 1.

2.5 DEFINITIES

De onderstaande definities zijn van toepassing, tenzij de context anders bepaalt:

Bestuurder heeft de betekenis die eraan gegeven wordt in artikel 2.1.

Code of Conduct heeft de betekenis die eraan gegeven wordt in artikel 2.1.

Datum van uitgifte verwijst naar de datum waarop de huidige Code of Conduct formeel voor de eerste keer goedgekeurd werd door de raad van bestuur van Gimv en vanaf wanneer hij van kracht werd voor alle Geadresseerden.

Datum van meest recente bijwerking verwijst naar de datum waarop de Code of Conduct gewijzigd werd na goedkeuring van de raad van bestuur van Gimv.

Effecten verwijst naar alle aandelen, schuldinstrumenten en alle derivaten en andere financiële instrumenten in de ruimste betekenis die hiermee verband houdt.

Geadresseerde heeft de betekenis die eraan gegeven wordt in artikel 2.1.

Gimv Compliance & ESG Office heeft de betekenis die eraan gegeven wordt in artikel 2.1.

Gimv Non-Trading List is het overzicht van beursgenoteerde Portefeuilleondernemingen waarvan de Effecten niet verhandeld mogen worden door de Geadresseerden en hun NVP's. Dat overzicht wordt bewaard en bijgewerkt door het Gimv Compliance & ESG Office en kan door alle Geadresseerden worden geraadpleegd op het intranet van Gimv.

Nauw Verbonden Persoon of ***NVP*** betekent, met betrekking tot een Geadresseerde:

i. een echtgenoot of echtgenote, of een wettelijk samenwonende partner;
ii. een kind dat wettelijk ten laste komt van de Geadresseerde (inclusief geadopteerde kinderen);
iii. een familielid dat op de datum van de transactie in kwestie gedurende ten minste één jaar deel uitmaakte van hetzelfde huishouden als de Geadresseerde; of
iv. een rechtspersoon, trust of personenvennootschap waarvan de leidinggevende verantwoordelijkheid berust bij de Geadresseerde of een persoon zoals bedoeld onder (i), (ii) of (iii), die rechtstreeks of onrechtstreeks onder de zeggenschap staat van de Geadresseerde of dergelijke persoon, die opgericht werd ten behoeve van de Geadresseerde of dergelijke persoon, of waarvan de economische belangen in wezen gelijkwaardig zijn aan die van de Geadresseerde of dergelijke persoon.

Portefeuilleonderneming staat voor elke entiteit waarin Gimv-groep een belang heeft (door middel van effecten of andere) als onderdeel van haar dagelijkse bedrijfsvoering.

Transactie moet worden geïnterpreteerd als elke transactie, in de ruimste betekenis, met betrekking tot Effecten.

Werknemer heeft de betekenis die eraan gegeven wordt in artikel 2.1.

3 INTERACTIES MET PORTEFEUILLEONDERNEMINGEN

3.1 BEURSGENOTEERDE PORTEFEUILLEONDERNEMINGEN

Werknemers, Bestuurders en hun Nauw Verbonden Personen (NVP's) mogen alleen Transacties verrichten in Effecten die worden uitgegeven door beursgenoteerde Portefeuilleondernemingen als die Transacties toegelaten zijn volgens het verhandelingsreglement van die beursgenoteerde Portefeuilleonderneming en op voorwaarde dat die beursgenoteerde Portefeuilleonderneming niet vermeld is op de Gimv Non-Trading List. De raad van bestuur kan in uitzonderlijke omstandigheden toelating geven voor een transactie in Effecten die worden uitgegeven door Portefeuilleondernemingen die vermeld worden op de Gimv Non-Trading List (bv. in geval van een erfenis).

3.2 NIET-BEURSGENOTEERDE PORTEFEUILLEONDERNEMINGEN

Het is een Werknemer of Bestuurder uitdrukkelijk verboden om rechtstreeks of onrechtstreeks Effecten van niet-beursgenoteerde Portefeuilleondernemingen te bezitten. Werknemers en Bestuurders zullen de nodige redelijke voorzorgen nemen om te voorkomen dat dergelijke belangen aangehouden worden door hun respectieve NVP's. Deze algemene verbodsbepaling geldt met uitzondering van elke uitdrukkelijke en schriftelijke vrijstelling die door de raad van bestuur goedgekeurd kan worden en die onderworpen is aan de voorwaarden van die goedkeuring.

3.3 VERGOEDINGEN VOOR BENOEMINGEN BINNEN PORTEFEUILLEONDERNEMINGEN

Voor alle duidelijkheid, dit artikel 3.3 is niet van toepassing op Bestuurders die een mandaat bekleden als lid of waarnemer van een raad van bestuur, toezichthoudend orgaan of adviserend

orgaan (onvolledige lijst van functies en bedrijfsorganen) van een beursgenoteerde Portefeuilleonderneming van Gimv.

Elke vergoeding, van eender welke aard, waarop Werknemers recht hebben krachtens een mandaat als lid of waarnemer van een raad van bestuur, toezichthoudend orgaan of adviserend orgaan (onvolledige lijst van functies en bedrijfsorganen) van een Portefeuilleonderneming van Gimv dient, bij voorkeur rechtstreeks door die Portefeuilleonderneming aan Gimv (of de hiertoe aangestelde entiteit van de Gimv-groep) te worden betaald. Ingeval dergelijke vergoeding betaald werd aan een Werknemer, zal de Werknemer de vergoeding onmiddellijk overmaken op een van de bankrekeningen van Gimv zoals vermeld op het briefpapier van Gimv.

Vergoedingen zoals bedoeld in dit artikel omvatten (niet-limitatief) variabele bestuurdersbezoldigingen, aanwezigheidsvergoedingen, salarissen, beheersvergoedingen, dienstverlenings- of consultancyvergoedingen en alle andere vergelijkbare vormen van vergoeding.

4 BUSINESS ETHIEK EN INTEGRITEIT

Het is de ambitie van Gimv om goed presterende bedrijven verder uit te bouwen en te doen groeien in aantrekkelijke groeimarkten door in te zetten op waardecreatie via strategie en businessmodellen, internationale expansie en operationele uitmuntendheid. In dit verband heeft Gimv haar visie op een duurzame toekomst van de economie en samenleving vertaald in vijf specifieke investeringsplatformen: Consumer, Healthcare, Life Sciences Smart Industries en Sustainable Cities.

Bij het realiseren van haar ambities, verwacht Gimv van haar Portefeuilleondernemingen en hun bestuurders, leidinggevenden, managers, werknemers en andere vertegenwoordigers hoge ethische normen, een continu voorbeeldig gedrag en een streven naar uitmuntendheid. Hiertoe dienen Gimv en haar Werknemers en Bestuurders de norm te bepalen op het vlak van respect, business ethiek en integriteit.

Bovendien engageert Gimv zich ertoe om alleen te werken met derde partijen (inclusief tussenpersonen en adviseurs) van wie het gedrag overeenstemt met de normen en waarden zoals hieronder uiteengezet.

4.1 VERANTWOORD INVESTEREN

Gimv is een toonaangevende, verantwoordelijke en maatschappijgerichte Europese private equity-onderneming. Daarom verbindt Gimv zich ertoe niet te investeren in alsook erover te waken dat haar portfolio-ondernemingen niet investeren in volgende bedrijven of activiteiten:

- waarvan de activiteiten, producten of diensten als illegaal worden beschouwd onder toepasselijke wetgeving, regulering of wereldwijde conventies in de relevante jurisdicties (inclusief maar niet beperkt tot slavernij, uitbuiting, dwangarbeid, mensenhandel, kinderarbeid, prostitutie, illegale substanties of welke vorm dan ook van georganiseerde misdaad);
- die betrokken zijn bij de productie, de verkoop, het gebruik van of de handel in wapens, massavernietigingswapens of onmenselijke wapens of essentiële onderdelen daarvan (inclusief maar niet beperkt tot nucleaire, chemische en radiologische wapens, landmijnen en bommen). Goederen, diensten of slimme technologieën en oplossingen die defensief of niet-aanvallend zijn in gebieden zoals luchtvaartelektronica, radar, sonar, instrumentatie, communicatie en bescherming (niet-uitputtend) kunnen in

overeenstemming zijn met het beleid inzake verantwoorde investeringen van Gimv na een passende beoordeling door het Gimv Compliance & ESG Office;
- waarvan de activiteiten rechtstreeks of onrechtstreeks bijdragen tot de financiering van terrorisme;
- die actief zijn in of betrokken bij de ontwikkeling, uitbating, verkoop, distributie, beheer van of handel in producten en/of diensten en/of faciliteiten die een rechtstreeks of onrechtstreeks verband houden met gokken, tabak of pornografie.

Bij twijfel of de activiteiten van een (mogelijke) Portefeuilleonderneming onder de bovengenoemde criteria vallen, neem dan gerust contact op met de Gimv Compliance & ESG Office.

Gimv verwacht van haar Portefeuilleondernemingen dat zij een toegewijde, constructieve en betrouwbare partner zijn die zich ertoe verbindt om:

- toepasselijke wetten, regelgevingen of wereldwijde verdragen te respecteren;
- het mededingingsrecht te respecteren in de omgang met concurrenten, leveranciers en klanten;
- nooit deel te nemen aan enige omkoping, corruptie of soortgelijk gedrag
- hoge normen en waarden op vlak van zakelijke integriteit te handhaven en zich op de juiste ethische wijze te gedragen, inclusief maar niet beperkt tot:
    - het voeren van een verantwoorde en duurzame aanpak op vlak van het beheer van de milieuaspecten van diens activiteiten;
    - het respecteren van de rechten van de werknemers, ze eerlijk behandelen en het waarborgen van een gezonde en veilige werkomgeving;
    - het invoeren van een gepaste cultuur op het gebied van governance, risicobeheer en compliance.

4.2 WERKOMGEVING

Alle Geadresseerden dienen de verschillen in de eigenheid van elke persoon die binnen Gimv als Werknemer of Bestuurder werkt, te respecteren. Alle Geadresseerden dienen elkaar derhalve te respecteren en de doelstellingen van Gimv samen te verwezenlijken zonder acht te slaan op ras, etniciteit, religie, herkomst, geslacht, seksuele geaardheid, handicap, leeftijd, burgerlijke staat of andere eigenschappen. Geen enkele vorm van ongeoorloofde discriminatie nog ongepast/onaanvaardbaar (seksueel) gedrag zal worden getolereerd.

Gimv hecht veel belang aan het creëren en in stand houden van een werkomgeving waarin mensen met waardigheid en respect behandeld worden en die gekenmerkt wordt door wederzijds vertrouwen en het ontbreken van enige (rechtstreekse of onrechtstreekse) vorm van intimidatie, onderdrukking en uitbuiting.

4.3 VERTROUWELIJKE INFORMATIE

Alle Geadresseerden hebben toegang of kunnen toegang hebben tot vertrouwelijke informatie over (i) Gimv, (ii) de activiteiten van Gimv als private equity-vennootschap die belegt in Portefeuilleondernemingen en (iii) (potentiële) Portefeuilleondernemingen van Gimv en derden. Alle Geadresseerden dienen dan ook de nodige voorzorgen te treffen om het vertrouwelijke karakter van die informatie te bewaren en elke ongeoorloofde openbaarmaking aan concurrenten of andere onbevoegde derden te voorkomen.

Om de integriteit en veiligheid van haar eigen gegevens te beschermen, heeft Gimv het Gimv Data Protection Framework opgezet om datalekken of onrechtmatige verliezen van binnenuit te

detecteren en te alarmeren. Een gedetailleerde beschrijving van hoe het Gimv Data Protection Framework werkt (inclusief hoe Gimv omgaat met mogelijke gevolgen voor de privacy van de werknemers) is toegevoegd aan de Code of Conduct als bijlage 3.

4.4 BELANGENCONFLICTEN

Belangenconflicten kunnen ontstaan wanneer er sprake is van een rechtstreeks of onrechtstreeks persoonlijk belang bij een beslissing die wordt genomen door en voor Gimv. Bij belangenconflicten is de onpartijdigheid van een beslissing niet gegarandeerd.

Bijgevolg zullen alle Geadresseerden, naast het toepassen van de regels van de Belgische Wetboek van Vennootschappen die van toepassing zijn op belangenconflicten van Bestuurders of leden van directiecomités, een rechtvaardig, objectief en niet-vooringenomen oordeel vormen bij alle zakelijke transacties van Gimv, waarbij het belang van Gimv altijd voorrang heeft op elk persoonlijk belang in de zakelijke aangelegenheden van Gimv.

Geadresseerden zullen hun positie niet gebruiken om een rechtstreeks of onrechtstreeks persoonlijk voordeel te bekomen en zullen het Gimv Compliance & ESG Office op de hoogte stellen van alle belangenconflicten, alsook elke andere relatie die ze hebben met een (potentiële) portefeuilleonderneming dan de relatie die ontstaat uit de dagelijkse bedrijfsvoering van Gimv, een derde-leverancier of consultant die voor Gimv of een concurrent van Gimv werkt. Het Gimv Compliance & ESG Office behoudt zich het recht voor om de raad van bestuur van Gimv op de hoogte te brengen van dergelijke gemelde belangenconflicten. Alle Geadresseerden moeten zich onthouden van elke betrokkenheid in eender welke transactie of bedrijfsactiviteit die beschouwd kan worden als of aanleiding kan geven tot een belangenconflict.

Ingeval een Geadresseerde niet weet of een bepaalde situatie al dan niet een belangenconflict vormt, wordt hij/zij aangemoedigd om contact op te nemen met het Gimv Compliance & ESG Office.

4.5 GEBRUIK VAN GIMV-MIDDELEN

Het is de Geadresseerden verboden om middelen, activa of kredieten van Gimv (of elke andere entiteit van de Gimv-groep) of een Portefeuilleonderneming te gebruiken voor andere doeleinden dan de gewone bedrijfsvoering van Gimv of voor onwettige doeleinden. Gimv begrijpt dat Werknemers af en toe tijdens de werkuren persoonlijke zaken moeten afhandelen die niet buiten de normale werkuren afgehandeld kunnen worden, waarbij het gebruik van de arbeidstijd niet overdreven mag worden. Bij twijfel kan de Werknemer eerst een goedkeuring vragen van zijn of haar departementshoofd.

Voor de richtlijnen in verband met het correcte gebruik van de IT-voorzieningen en -omgeving van Gimv verwijzen we naar de afzonderlijke IT-policy die toegevoegd werd aan deze Code of Conduct als bijlage 5 en ook geraadpleegd kan worden op het intranet van Gimv.

4.6 EERLIJKE CONCURRENTIE

Gimv hecht veel belang aan eerlijke concurrentie en wenst haar bedrijfsactiviteiten ethisch en met integriteit uit te oefenen. Daarom houdt Gimv zich niet bezig en zal het zich nooit bezighouden met investeringen of zakelijke afspraken die de concurrentie verstoren, uitschakelen of ontmoedigen of die haar oneerlijke concurrentievoordelen verschaffen.

4.7 GIFTEN EN OMKOPING

Gimv is een commercieel actieve onderneming en handelt met haar Portefeuilleondernemingen, consultants, dienstverleners en alle andere partijen dan ook volgens de redelijke en gangbare handelspraktijken. Giften en gunsten, alsook occasionele maaltijden die worden aangeboden of aanvaard door Geadresseerden worden bijgevolg beschouwd als zijnde in overeenstemming met de redelijke en gangbare handelspraktijken wanneer ze bescheiden (in waarde en frequentie) en gepast (zowel tijd als plaats) zijn. De uitwisseling van cash geld en equivalenten wordt in geen geval aanvaard.

In ieder geval verbiedt Gimv formeel steekpenningen en giften die worden uitgedeeld, aangeboden of aanvaard en die dienen om zakelijke of andere ongepaste voordelen of beloften te bekomen of in stand te houden. Het verhullen van giften of entertainment als schenkingen aan liefdadigheidsinstellingen wordt, tot slot, beschouwd als een schending van de Code of Conduct.

Ingeval een Geadresseerde niet zeker is of een bepaalde situatie al dan niet onder de redelijke en gangbare handelspraktijken valt, dient hij/zij contact op te nemen met het Gimv Compliance & ESG Office.

Gimv kan te allen tijde actie ondernemen (met inbegrip van gerechtelijke procedures) tegen Werknemers, Bestuurders, (potentiële) Portefeuilleondernemingen, consultants of dienstverleners (niet-uitputtend) die zich schuldig maken of schuldig zijn aan (medeplichtigheid aan) omkoping, fraude, prijsafspraken, factureringen voor diensten die ze niet verleenden, corruptie of poging tot corruptie.

5 EXTERNE COMMUNICATIE EN SOCIALE MEDIA

De voorzitter, de CEO, de overige leden van het executief comité en elke andere persoon specifiek daartoe aangeduid zijn de enige verantwoordelijken voor de externe communicatie van Gimv en voor het onderhouden van contacten met de media. Bijgevolg dienen alle vragen van de media (in eender welke vorm) onmiddellijk te worden doorgegeven aan een van voormelde personen.

Alle Geadresseerden moeten bijdragen tot het beschermen en verbeteren van het imago van Gimv. Bijgevolg moeten alle Geadresseerden zich bewust zijn van wat ze over Gimv schrijven op websites, blogs of sociale media met inbegrip van maar niet beperkt tot Facebook, Twitter en LinkedIn. Gimv heeft enkele interne sociale media richtlijnen ter beschikking gesteld van haar werknemers op het Gimv Intranet.

6 WETTEN EN REGELS

Zaken doen in overeenstemming met de hoogste ethische normen en waarden brengt uiteraard ook respect voor de rechtsstaat en naleving van geldende wetgeving met zich mee. Elke overtreding van een wet of regelgeving kan resulteren in sancties van burgerrechtelijke, administratieve of strafrechtelijke aard die worden opgelegd aan Gimv en de betrokken Geadresseerde. Dat kan negatieve gevolgen hebben voor de loopbaan van de Geadresseerde in kwestie. In geval van vragen over de toepasselijke wetgeving, neem contact op met het Legal departement of het Gimv Compliance & ESG Office.

BIJLAGE 1
BEVESTIGING VAN ONTVANGST

Aan: Gimv nv

Karel Oomsstraat 37

2018 Antwerpen

België

(hierna de ***Vennootschap***)

Ik bevestig hierbij dat ik de Gimv Code of Conduct inclusief haar bijlagen (i.e. de Gimv Whisleblowing Policy, het Gimv Data Protection Framework, de Gimv Expense Polocy en de Gimv IT-Policy) samen met dit formulier ontvangen heb.

Ik bevestig dat ik de Code of Conduct en haar bijlagen, zoals van tijd tot tijd gewijzigd, heb gelezen, begrepen en zal naleven.

Handtekening:……..

Datum:……

Gelieve dit formulier in te vullen en te bezorgen aan het Gimv Compliance Office per e-mail compliance@gimv.com.

BIJLAGE 2
GIMV WHISTLEBLOWING POLICY
(KLOKKENLUIDERSBELEID)

Gimv nv
Karel Oomsstraat 37, 2018 Antwerpen, België
T +32 3 290 21 00 | **F** +32 3 290 21 05
www.gimv.com

WHISTLEBLOWING POLICY

(KLOKKENLUIDERSBELEID)

INHOUDSOPGAVE

ACHTERGROND

Gimv NV is een naamloze vennootschap naar Belgisch recht met maatschappelijke zetel te 2018 Antwerpen, Karel Oomsstraat 37, België en ingeschreven bij de Kruispuntbank voor Ondernemingen onder nummer 0220.324.117 (hierna "**Gimv**" of de "**Vennootschap**").

Gimv legt zich toe op de hoogste normen van openheid, integriteit, transparantie en rekenschap. Een belangrijk aspect van deze waarden is om alle aandeelhouders, leden van het management, vaste, tijdelijke en voormalige personeelsleden, agenten, onderaannemers en andere gelieerde ondernemingen[1] (hierna individueel aan te duiden als een "**Geadresseerde**" en gezamenlijk de "**Geadresseerden**") van Gimv en haar dochterondernemingen (hierna **"Gimv-groep"**) een effectieve procedure te bieden om kwesties aan te kaarten die in dit Klokkenluidersbeleid (het "**Klokkenluidersbeleid"**) zijn opgesomd. Voor alle duidelijkheid: dochterondernemingen omvatten niet de externe portefeuillebedrijven van Gimv-groep, noch TDP, TINC en door TDP beheerde fondsen.

"**Klokkenluiden**" is het proces waarbij een individu te goeder trouw oprechte bezorgdheid uit over zaken die binnen Gimv ernstige zorgen lijken te impliceren.

Gimv erkent de waarde van de melding door de Geadresseerde van bezorgdheden over Gimv's activiteiten en operaties (in een dergelijk geval wordt de Geadresseerde gekwalificeerd als een "**Klokkenluider"**).

Gimv moedigt Geadresseerden daarom aan om dergelijke zorgen intern te uiten door indien nodig een melding te doen (een dergelijke melding is een "**Klokkenluidersmelding"**).

In lijn met zijn eigen engagement vertrouwt Gimv erop dat alle Geadresseerden het melden zullen zien als een positieve bijdrage aan de bescherming en verbetering van de werkcultuur, de reputatie en het succes van Gimv. Alle Geadresseerden hebben de verantwoordelijkheid om verdachte activiteiten onmiddellijk en in overeenstemming met dit Klokkenluidersbeleid te melden.

Het doel van dit Klokkenluidersbeleid is om een kader en een procedure te bieden voor Geadresseerden om intern "de klok te luiden" over interne inbreuken op wet- en regelgeving en de naleving van de voorschriften of ethische inbreuken. Het beschrijft de procedure waarmee dergelijke zorgen kunnen worden geuit en waarop actie kan worden ondernomen. Voorts wordt gedetailleerd aangegeven wanneer en hoe bescherming tegen represailles van toepassing is, alsook hoe vertrouwelijkheid, belangenconflicten en wettelijk voorrecht (indien van toepassing) moeten worden beheerd.

De doelstellingen van dit Klokkenluidersbeleid zijn te waarborgen dat:

- De Geadresseerden duidelijk weten wanneer en hoe zij zich moeten uitspreken en een Klokkenluidersmelding moeten indienen;
- De Geadresseerden een duidelijk inzicht hebben in de interne functies en de stappen die worden ondernomen om de onafhankelijkheid en doeltreffendheid van de Klokkenluidersprocedure te waarborgen;
- Gimv in staat is om tijdig en doeltreffend op te treden tegen Te Melden Bezorgdheden.

[1] Dit omvat alle werknemers in een professionele context, huidige en voormalige leden, alsook personen die betrokken zijn bij een rekruteringsproces, d.w.z. werknemers, zelfstandigen, vrijwilligers, (onbezoldigde) stagiairs, aandeelhouders, leden van bestuurs-, administratieve of toezichthoudende organen van Gimv.

DEEL 1. TE MELDEN BEZORGDHEDEN

Gimv moedigt alle Geadresseerden aan om een Klokkenluidersmelding in te dienen wanneer zij **een redelijke en legitieme overtuiging** hebben dat schendingen worden, zijn of waarschijnlijk zullen worden begaan met betrekking tot:

- Overheidsopdrachten;
- Financiële diensten, producten en markten, voorkoming van witwassen van geld en terrorismefinanciering;
- Productveiligheid en productconformiteit;
- Veiligheid van het vervoer;
- Bescherming van het milieu;
- Stralingsbescherming en nucleaire veiligheid;
- Veiligheid van levensmiddelen en diervoeders, diergezondheid en dierenwelzijn;
- Volksgezondheid;
- Consumentenbescherming;
- Bescherming van de persoonlijke levenssfeer en persoonsgegevens, en beveiliging van het netwerk- en het informatiesystemen;
- Niet-naleving van de antitrust- of mededingingswetgeving;
- Een inbreuk waardoor de financiële belangen van de Europese Unie worden geschaad[2] ;
- Een inbreuk op het beleid en de procedures van Gimv[3] ;

(een dergelijke situatie wordt hierna omschreven als een "Te Melden Bezorgdheid**"**).

Dit Klokkenluidersbeleid heeft **geen** betrekking op klachten die specifiek zijn voor de arbeidsomstandigheden, met inbegrip van, maar niet beperkt tot sociale, arbeids- en werkgelegenheidsklachten, die moeten worden behandeld in overeenstemming met de toepasselijke HR-procedures, en waarvoor geen Klokkenluidersmelding moet worden ingediend.

Geadresseerden hebben geen verantwoordelijkheid voor het onderzoeken van de zaak die zij (willen) melden. Het is de verantwoordelijkheid van Gimv om ervoor te zorgen dat er een onderzoek plaatsvindt na ontvangst van de Klokkenluidersmelding.

[2] met betrekking tot de bestrijding van fraude, corruptie en elke andere onwettige activiteit waardoor de uitgaven van de Unie, de inning van ontvangsten en middelen van de Europese Unie of het vermogen van de Europese Unie worden aangetast.

[3] Het beleid en de procedures van Gimv zijn niet alleen opgesteld om te voldoen aan wettelijke en specifieke verplichtingen, maar ook om de juiste richtlijnen te weerspiegelen en goede praktijken en een cultuur te bevorderen die het succes van Gimv ondersteunen.

DEEL 2. PRINCIPES

Geadresseerden moeten altijd handelen in overeenstemming met de volgende algemene beginselen:

- Te melden bezorgdheden moeten altijd te goeder trouw worden gemeld; dit laatste wordt verondersteld;
- Te melden bezorgdheden kunnen ook zonder ondersteunend bewijs worden gemeld: voldoende overtuiging dat een Te Melden Bezorgdheid plaatsvindt of op het punt staat plaats te vinden, is voldoende;
- Alleen rechtstreeks te melden bezorgdheden mogen worden gemeld en er mogen geen "van horen zeggen"-verklaringen worden afgelegd;
- Te melden bezorgdheden mogen geen wraakzuchtige of persoonlijke doeleinden dienen (wat vermoedelijk als melding te kwader trouw kan worden aangemerkt);
- Te melden bezorgdheden kunnen op naam of anoniem worden gemeld;
- Van de rechten en bescherming die in dit Klokkenluidersbeleid zijn vastgelegd, kan geen afstand worden gedaan door middel van een overeenkomst, beleid, formulier of arbeidsvoorwaarde.

DEEL 3. BESCHERMING VAN KLOKKENLUIDERS

1. Bescherming voor melding *te goeder trouw*

Gimv zal elke Geadresseerde die *te goeder trouw* een Klokkenluidersmelding heeft gedaan, zelfs als deze onjuist blijkt te zijn, beschermen tegen ontslag en elke andere vorm van represailles, bedreiging of vijandige actie.

Verboden vergeldingsmaatregelen omvatten, maar zijn niet beperkt tot, schorsing, ontslag of soortgelijke maatregelen, demotie of het onthouden van promotie, overplaatsing van taken, verandering van werklocatie, loonsverlaging, het onthouden van opleiding, discriminatie, dwang, intimidatie, pesterijen, ...

Elke vorm van dergelijke vergeldingsmaatregelen kan leiden tot disciplinaire maatregelen in overeenstemming met de toepasselijke regels en het beleid van Gimv, tot en met beëindiging van het dienstverband, alsook de verwijzing naar gerechtelijke instanties.

Deze bescherming wordt ook geboden aan Klokkenluiders die informatie doorgeven die zij buiten een beroepscontext hebben verkregen.

Een dergelijke bescherming wordt in voorkomend geval ook verleend aan facilitators, collega's of familieleden van de Klokkenluider die ook in een werkgerelateerde band staan met de werkgever van de Klokkenluider of diens klant of afnemer van diensten, en elke juridische entiteit waarvan de Klokkenluider eigenaar is, waarvoor hij werkt, of waarmee hij anderszins in een werkgerelateerde context verbonden is.

Klokkenluiders zijn niet aansprakelijk voor het verkrijgen van of het zich toegang verschaffen tot te melden informatie, mits het verkrijgen van of het zich toegang verschaffen tot dergelijke informatie geen afzonderlijk strafbaar feit vormt.

2. Geen bescherming bij melding *te kwader trouw*

Gimv neemt elke aangifte waarvan *geweten is dat ze vals is* of die *te kwader trouw*, kwaadwillig, roekeloos of met het oog op persoonlijk gewin gebeurt, zeer ernstig.

Indien uit het onderzoek blijkt dat een Geadresseerde te kwader trouw een Klokkenluidersmelding heeft ingediend, kan Gimv disciplinaire maatregelen nemen tegen de Klokkenluider in overeenstemming met zijn toepasselijke regels en beleid, tot en met beëindiging van het dienstverband, alsook doorverwijzing naar gerechtelijke instanties.

DEEL 4. VERTROUWELIJKHEID

Een Klokkenluidersmelding kan op naam of anoniem worden ingediend.

Dit Klokkenluidersbeleid garandeert dat alle meldingen van Klokkenluiders onmiddellijk, onafhankelijk en grondig zullen worden behandeld, zonder enige schade te berokkenen aan de Geadresseerden, hun carrière of reputatie. Gimv zal in alle gevallen de vertrouwelijkheid en identiteit beschermen van Klokkenluiders en andere partijen die betrokken zijn bij de melding en het daaropvolgende interne onderzoek, indien van toepassing. De persoon die verantwoordelijk is voor de behandeling van de Klokkenluidersmelding zal optreden als verantwoordelijke voor de bescherming van de identiteit.

Van alle partijen die bij het onderzoek en de daaropvolgende procedures betrokken zijn, wordt volledige discretie verwacht.

Dit Klokkenluidersbeleid voorkomt ook dat niet-gemachtigd personeel toegang krijgt tot de gemelde informatie.

De identiteit van de Klokkenluider en andere relevante personen kan alleen worden opgeheven in een van de volgende uitputtende gevallen:

- Met de uitdrukkelijke toestemming van de personen wier identiteit wordt beschermd, in de wetenschap dat de Klokkenluider zichzelf op elk moment kan identificeren;
- Op verzoek van bevoegde gerechtelijke of regelgevende instanties, voor zover Gimv wettelijk verplicht is met deze instanties samen te werken;
- Indien de Te Melden Bezorgdheid wordt gebruikt in het kader van een gerechtelijke procedure;
- Als je advies vraagt aan een accountant of een advocaat;
- Als de informatie al in het publieke domein is,

in gedachten te houden dat dit Klokkenluidersbeleid in de eerste plaats tot doel heeft Klokkenluiders te goeder trouw te beschermen tegen disciplinaire maatregelen, vergeldingsmaatregelen of aantasting van de reputatie of het vertrouwen.

DEEL 5. INTERNE RAPPORTAGE

Interne rapportagekanalen verdienen de voorkeur boven externe rapportage, waarvoor specifieke voorwaarden gelden (zie **DEEL 6.** hieronder).

1. Klokkenluidersmanager

Gimv heeft de interne verantwoordelijkheid voor de behandeling (d.w.z. het ontvangen en opvolgen) van Klokkenluidersmeldingen, met inbegrip van het uitvoeren van onderzoeken en het aanbevelen van verdere acties waar nodig, toevertrouwd aan de Gimv Compliance & ESG Office. Onder de leden van de Gimv Compliance & ESG Office is de Compliance Manager van Gimv aangeduid als de "**Klokkenluidersmanager"**.

De aanstelling van een speciale Klokkenluidersmanager garandeert dat de zaak wordt behandeld overeenkomstig de governance-beginselen inzake bekwaamheid, zorgvuldigheid, billijkheid en onpartijdigheid.

2. Indienen van een Klokkenluidersmelding

Klokkenluidersmeldingen moeten per e-mail worden ingediend bij de Klokkenluidersmanager, met inachtneming van de richtlijnen voor Klokkenluiders in **BIJLAGE 1**.

Bij wijze van uitzondering, wanneer het niet gepast is dat de Klokkenluidersmanager het onderzoek voert (bv. wegens belangenconflict, ook wanneer de Klokkenluidersmanager het onderwerp van de melding is), kan de Klokkenluidersmelding worden ingediend bij een van de andere leden van de Gimv Compliance & ESG Office, waaronder de CEO, CFO en CLO - Secretaris-Generaal of eveneens de voorzitter van de raad van bestuur van Gimv.

3. Ontvangstbevestiging

De Klokkenluidersmanager moet de ontvangst van de melding binnen zeven (7) werkdagen na indiening bevestigen aan de Klokkenluider (tenzij de melding anoniem is gedaan).

De Klokkenluidersmanager geeft bij deze gelegenheid aan, indien van toepassing en voor zover mogelijk, of de Klokkenluidersmelding binnen de werkingssfeer van het Klokkenluidersbeleid valt en derhalve ontvankelijk wordt geacht, met inbegrip van de rechten en plichten die aan een dergelijke melding zijn verbonden en de stappen die vervolgens moeten worden ondernomen. Ook wordt verduidelijkt dat op verzoek van de Klokkenluider een bijeenkomst kan worden geregeld.

4. Ontvankelijkheid

Na ontvangst van een Klokkenluidersmelding gaat de Klokkenluidersmanager na of de melding ontvankelijk is:

- De gerapporteerde feiten vallen binnen het toepassingsgebied van het Klokkenluidersbeleid, d.w.z. dat er sprake is van een Te Melden Bezorgdheid;

- De melder valt binnen de werkingssfeer van het Klokkenluidersbeleid, d.w.z. hij/zij komt in aanmerking als Klokkenluider; en
- Aan de formele vereisten voor een Klokkenluidersmelding is voldaan.

5. Voorlopige beoordeling van het Klokkenluidersmelding

Indien toelaatbaar, maakt de Klokkenluidersmanager een primaire beoordeling van de informatie in de Klokkenluidersmelding om de materialiteit ervan te bepalen, inclusief:

- De regels, verplichtingen, gedragingen of normen die zouden zijn geschonden;
- De onderliggende feiten die tot verslaggeving leiden;
- De naam, functie en positie van de personen die verantwoordelijk zouden zijn voor de te melden zaak;
- De naam, positie en functie van de Klokkenluider (indien van toepassing) en eventuele andere betrokken personen.

Om aan deze verplichting te voldoen, zal de Klokkenluidersmanager een follow-up formulier voor Klokkenluidersmeldingen invullen.

6. Intern onderzoek

De Klokkenluidersmanager moet tijdig en met de nodige zorgvuldigheid handelen en alle beschikbare maatregelen nemen om een intern onderzoek in te stellen en de gemelde inbreuk (indien van toepassing) te verhelpen, ongeacht of de Klokkenluidersmelding nominatief of anoniem is ingediend.

De Klokkenluidersmanager kan te allen tijde contact opnemen met de Klokkenluider, indien nodig, om deze beoordeling uit te voeren.

De Klokkenluidersmanager moet in elk geval zorgen voor follow-up en feedback aan de Klokkenluider over acties of het gebrek daaraan binnen een redelijke termijn, gezien de noodzaak om het probleem dat het onderwerp is van de Klokkenluidersmelding onmiddellijk aan te pakken.

Deze termijn mag niet langer zijn dan drie (3) maanden, maar kan worden verlengd tot zes (6) maanden indien de specifieke omstandigheden van het geval, met name de aard en de complexiteit van het onderwerp van de Klokkenluidersmelding, zulks vereisen dat een langdurig onderzoek wordt ingesteld.

DEEL 6. EXTERNE VERSLAGGEVING

1. Rapportering aan de bevoegde autoriteit

De Klokkenluider kan een Te Melden Bezorgdheid delen met een bevoegde externe regelgevende instantie of autoriteit, inclusief strafrechtelijke autoriteiten, **op voorwaarde dat**:

- *Na interne rapportage*: hij/zij niet tevreden is met het resultaat van de interne procedure - ook indien er geen follow-up is geweest van de interne rapportage binnen de hieronder aangegeven termijn; *of*
- *Rechtstreeks, d.w.z. zonder interne melding*: als hij/zij vreest dat hun bezorgdheid intern niet op een correcte, onafhankelijke en objectieve manier zal worden behandeld. De Klokkenluider moet de situatie echter zorgvuldig onderzoeken alvorens te besluiten rechtstreeks een externe melding te doen, aangezien interne melding altijd de voorkeur verdient.

2. Openbaarmaking

Klokkenluiders hebben het recht om een openbare bekendmaking te doen[4] en in aanmerking te komen voor de in de procedure vastgestelde rechten en bescherming, **op voorwaarde dat**:

- De Klokkenluider de zaak eerst zowel intern als extern gemeld heeft, of extern aan de bevoegde regelgevende instantie of autoriteit, maar er is geen passende actie ondernomen in reactie op een dergelijke melding binnen het hierboven gespecificeerde tijdsbestek **(DEEL 5**, **Sectie 3**); of
- De Klokkenluider redelijke gronden heeft om aan te nemen dat:
  - de inbreuk een onmiddellijk of duidelijk gevaar voor het openbaar belang kan vormen, bijvoorbeeld in geval van een noodsituatie of een risico van onomkeerbare schade; of
  - In het geval van externe melding bestaat het risico op vergelding of is de kans klein dat de inbreuk doeltreffend wordt aangepakt wegens de bijzondere omstandigheden van het geval, bijvoorbeeld wanneer bewijsmateriaal kan worden verborgen of vernietigd of wanneer een instantie kan samenspannen met de pleger van de inbreuk of bij de inbreuk betrokken kan zijn.

De Klokkenluider moet het kanaal van de openbare bekendmaking slechts als **laatste redmiddel** gebruiken**, en alleen** als aan de bovenstaande voorwaarden is voldaan.

Klokkenluiders zijn zich ervan bewust dat zij de in deze procedure gewaarborgde rechten en bescherming kunnen **verliezen** in geval van misbruik van het publieke meldingskanaal[5] .

[4] D.w.z. via sociale netwerken, persberichten, openbare interviews of andere kanalen met een vergelijkbaar effect.

[5] Klokkenluiders die overeenkomstig deze procedure en dit beleid gebruik maken van openbare meldingskanalen, worden niet geacht een beperking op de openbaarmaking van informatie te hebben overtreden en kunnen op geen enkele wijze aansprakelijk worden gesteld voor dergelijke openbaarmakingen.

DEEL 7. OPLEIDING

De Klokkenluidersmanager is er verantwoordelijk voor dat de Geadresseerden een passende opleiding krijgen over dit Klokkenluidersbeleid, dat zij hun plichten, rechten en bescherming begrijpen en zich daarvan bewust worden, voor zover van toepassing.

Er moeten voortdurend opleidingen worden gegeven, zowel bij de aanwerving van nieuwe werknemers als op gezette tijden wanneer dat nodig is.

Eens in de twee jaar controleert de Klokkenluidersmanager of alle Geadresseerden voldoende zijn opgeleid in dit Klokkenluidersbeleid.

De Klokkenluidersmanager doet periodieke mededelingen, indien nodig, om de Geadresseerden bewust te maken van dit Klokkenluidersbeleid.

DEEL 8. BIJHOUDEN VAN REGISTERS EN PRIVACY VAN GEGEVENS

Gimv heeft een klokkenluidersregister (het **Register**) ingevoerd om elke melding bij te houden die intern wordt ingediend, ongeacht of ze ontvankelijk is of niet. Dit Register wordt beheerd onder de controle en het toezicht van de Klokkenluidersmanager.

Het Register vermeldt:

- De datum en het tijdstip van de melding;
- De aard van de melding;
- De regels, verplichtingen, gedragingen of normen die zouden zijn geschonden;
- Een samenvatting van de onderliggende feiten die tot de melding hebben geleid;
- De naam, functie en rang van de personen die verantwoordelijk zijn voor de inbreuk;
- De naam, functie en positie van de Klokkenluider (indien van toepassing);
- De functie en positie van andere betrokken partijen;
- De stappen die zijn ondernomen na de indiening van de melding (in het kader van de onderzoeksprocedure);
- De conclusie over de waarheidsgetrouwheid en de materialiteit van de gemelde feiten en Te Melden Bezorgdheid;
- De maatregelen die zijn genomen op basis van de conclusie van de onderzoeksprocedure;
- Alle andere relevante elementen.

De dossiers moeten gedurende vijf (5) jaar na de oplossing van de zaak worden bewaard.

Gimv zorgt ervoor dat alle persoonsgegevens die worden verzameld naar aanleiding van dit Klokkenluidersbeleid, inclusief als onderdeel van het indienen van een melding, onderzoek en gerelateerde procedure, worden verwerkt met betrekking tot de naleving van de toepasselijke wetgeving en verplichtingen inzake gegevensprivacy. Dit omvat Verordening (EU) 2016/679 van 27 april 2016 (de GDPR) *en* de Belgische wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens, evenals het privacybeleid van Gimv**.**

Gimv zorgt er ook voor dat het het hoogste niveau van beveiliging biedt met betrekking tot de bescherming van gevoelige gegevens (indien aanwezig).

DEEL 9. TOEZICHT OP EN UITVOERING VAN DE PROCEDURE

1. Uitvoering

Dit Klokkenluidersbeleid is goedgekeurd door de Raad van Bestuur. De Klokkenluidersmanager heeft de primaire en dagelijkse verantwoordelijkheid voor de effectieve uitvoering van dit Klokkenluidersbeleid.

2. Toezicht

De Klokkenluidersmanager moet het gebruik en de doeltreffendheid van het Klokkenluidersbeleid voortdurend controleren, en het beleid zo nodig herzien en bijwerken. Eventuele verbeteringen aan het Klokkenluidersbeleid moeten zo snel mogelijk worden aangebracht, maar ten minste jaarlijks. Opmerkingen, suggesties en vragen met betrekking tot dit Klokkenluidersbeleid moeten worden gericht aan de Klokkenluidersmanager.

BIJLAGE 1: RICHTLIJNEN VOOR HET MELDEN VAN KLOKKENLUIDEN VOOR HET PERSONEEL

Als u een Te Melden Bezorgdheid aan Gimv wilt melden, kunt u uw Klokkenluidersmeldingen per e-mail rechtstreeks naar de Klokkenluidersmanager sturen op het volgende adres: compliance@gimv.com.

Vermeld ten minste de volgende gegevens in uw e-mail om uw Klokkenluidersmelding ontvankelijk te maken:

- De onderliggende feiten die tot de melding hebben geleid, inclusief maar niet beperkt tot:
  - *De feiten/gebeurtenissen waarvan u getuige was of waarvan u vermoedt dat ze hebben plaatsgevonden*
  - *De omstandigheden waarin de feiten/gebeurtenissen plaatsvonden (setting, context, data...)*
  - *Of het nu gaat om een voortdurend wangedrag/overtreding of een eenmalige gebeurtenis*
- De identiteit, functies en contactgegevens van de personen die het voorwerp uitmaken van de melding (d.w.z. de vermoedelijke overtreder);
- Bij nominatieve melding, uw identiteit, functies, en contactinformatie.

Gelieve *bij* uw e-mail ook documenten *te voegen* die de gerapporteerde bezorgdheid staven en/of bewijzen.

U moet uw volledige medewerking verlenen en alle relevante informatie verstrekken waar Gimv om verzoekt naar aanleiding van de indiening van een Klokkenluidersmelding (indien deze op persoonlijke titel gebeurt) en gedurende het interne onderzoek (indien dit plaatsvindt).

U moet in dit verband altijd uw geheimhoudingsplicht en loyaliteit tegenover Gimv in acht nemen.

U hebt het recht om uw Klokkenluidersmelding anoniem in te dienen. Echter, als u besluit anoniem te blijven:

- U ontvangt geen ontvangstbevestiging of feedback over uw Klokkenluidersmelding;
- De Klokkenluidersmanager zal niet in staat zijn om contact met u op te nemen om aanvullende informatie of ondersteunend bewijs te verkrijgen om uw melding en het onderzoek (indien van toepassing) te onderbouwen.

Zorg er daarom voor dat u zo veel mogelijk specifieke en gedetailleerde informatie en ondersteunende documentatie verstrekt, zodat de Klokkenluidersmanager de situatie adequaat kan beoordelen en uw Klokkenluidersmelding kan opvolgen.

BIJLAGE 3
GIMV DATA PROTECTION FRAMEWORK

Gimv nv
Karel Oomsstraat 37, 2018 Antwerpen, België
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

BIJLAGE 4
GIMV EXPENSE POLICY

Gimv nv
Karel Oomsstraat 37, 2018 Antwerpen, België
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.

BIJLAGE 5
GIMV IT USER POLICY

Gimv nv
Karel Oomsstraat 37, 2018 Antwerpen, België
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:	16/05/2023
Version number:	5.0
Status:	Final
Owner:	IT department

Policy reviewers

Name	Function
Creemers Johan	IT Manager
Sellenslagh Laura	Paralegal & Compliance Assistant
Van Bueren Vincent	Corporate Communications & Sustainability Manager
Vande Capelle Kristof	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.

1. Introduction

The purpose of this policy is to clarify the responsibilities of all Gimv employees to ensure the confidentiality, integrity and availability of Gimv information and information processing facilities. This document clarifies which actions can be taken if employees are not compliant with the applicable rules as defined in this policy and the Labour Standard (see 5. Compliance).

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.
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.
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. Acceptable use of assets

4.1.1 All IT devices and information stored on electronic and computing devices provisioned to the employee remains property of Gimv and shall only be used in the context of the execution of the Labour Standard and this policy.

4.1.2 The employee 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 employee shall only use IT devices provided by Gimv or validated by Gimv to access company networks.

4.1.4 Employees 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 employee 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 employee shall upon request by the IT department return the IT device at any time for inspection and/or audit.

4.1.7 The employee shall upon leaving Gimv, depending on the agreement with the employee, 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 employee 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 employee 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 employee shall keep the IT devices updated at all times.

4.2.3 The employee shall 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 employee 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 employee 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 employee shall not distribute, change or delete software provided by Gimv.

4.3. Controls against malicious activities

4.3.1 The employee shall immediately report any suspected information security event or incident to the IT department.
4.3.2 The employee 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 employee shall not make changes to system settings that prevent system updates from being installed.
4.3.4 The employee shall not open files or attachments from an unknown, suspicious or untrustworthy source.

4.4. Accounts and user credentials

4.4.1 The employee shall always use a password or Personal Identification Number (PIN) to protect IT devices from unauthorised access.
4.4.2 The employee shall change password upon first use.
4.4.3 The employee 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 (i.e., KeePass[2]) to keep user credentials secure. Please contact the IT department for more information.
4.4.4 The employee shall only use own username and password to login to information systems of Gimv and never share password with others (incl. staff, third parties or the IT department).
4.4.5 The employee shall adhere to the minimal set of requirements when creating a new password[2].
4.4.6 The employee 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 employee shall notify the IT department when the confidentiality of secret authentication information was or is thought to be compromised (see also 5.3.1).
4.4.8 The employee shall not use their business account for private purposes (e.g., use business credentials for LinkedIn) or use business credentials for private purposes.
4.4.9 The employee shall not enter login details when others are watching (i.e., “shoulder surfing”).
4.4.10 The employee should not use the “remember password” feature in a browser unless it is the extension from a password vault.
4.4.11 The employee should not re-use the same password for multiple accounts.

4.5. Secure transfer of information

4.5.1 The employee 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 employee shall 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 employee 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 employee shall always verify the correct recipient email address(es) are entered when sending emails so that confidential information is not compromised.
4.5.5 The employee shall securely store confidential printed material (i.e., clean desk) and ensure it is correctly destroyed when no longer needed.

4.5.6 The employee shall collect printed documents immediately from the printer and use the secure print function[2] where possible.
4.5.7 The employee shall 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.
4.5.8 The employee shall 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 shall 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 employee shall never store confidential information in public or private cloud services. If in doubt, please contact the IT department (see also: 5.5.1).

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: 5.6.5).
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 employee shall 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 employee shall 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 employee shall destroy printed documents containing confidential information using available methods, such as a shredder.
4.6.5 The employee shall 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 employee shall 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 employee shall 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 employee shall sign visitors in and out with arrival and departure times and visitors are required to wear an identification badge. For secure areas visitors shall be accompanied all the time.

4.8. Information security awareness, education and training

4.8.1 The employee 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.

4.8.2 The employee shall follow trainings provided by the IT team if and when.

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.