Politikk for den interne europeiske informasjonskanalen

Godkjent av styret i
TEKA INDUSTRIAL, S.A.

Politikk for den interne europeiske informasjonskanalen Midea & Teka Europe

1. Innledning og formål

Teka Industrial, S.A., dets datterselskaper og de europeiske enhetene i Mideas hvitevareavdeling er en del av Midea Group Co. Ltd. («Midea Group»). Midea Group forplikter seg til å drive sin virksomhet i alle regioner med integritet og i samsvar med loven.

I den europeiske regionen er det implementert en intern informasjonskanal i samsvar med kravene i lov 2/2023 av 20. februar, som regulerer beskyttelsen av personer som rapporterer om brudd på regelverket og bekjempelse av korrupsjon, og som gjennomfører direktiv (EU) 2019/1937 av Europaparlamentet og Rådet av 23. oktober 2019 om beskyttelse av personer som melder fra om brudd på unionsretten (heretter **«direktivet»**), samt forordning (EU) 2016/679 og lov 3/2018 om beskyttelse av personopplysninger og sikring av digitale rettigheter. Den interne europeiske varslingskanalen integrerer alle varslingskanaler i Europa, og anvendelsesområdet omfatter Teka Industrial, S.A., alle dets datterselskaper i Europa og Mideas hvitevareenheter i Europa og Storbritannia, som angitt **i vedlegg II.**

Formålet med denne policyen er å tilby en klagekanal som er tilgjengelig for Den europeiske union (inkludert Storbritannia) (heretter «den **interne europeiske** informasjonskanalen»), og den er utformet, etablert og administrert på en slik måte at den muliggjør: i) tilgjengelig bruk; ii) innlevering av skriftlige og/eller muntlige meldinger; (iii) overholdelse av garantier for konfidensialitet og anonymitet, unntatt i tilfeller hvor offentliggjøring er foreskrevet i nasjonal lovgivning eller kreves i forbindelse med en rettssak; iv) beskyttelse mot represalier; v) effektiv håndtering av meldinger og tilstrekkelig oppfølging av disse; vi) integrering av de ulike varslingskanalene i Europa (inkludert Storbritannia) og vii) beskyttelse av personopplysninger.

Den interne europeiske informasjonskanalen er beregnet på ansatte og tredjeparter i alle selskaper som er oppført i **vedlegg II**, og administreres av Teka Industrial, S.A. i Spania med støtte fra systemansvarlig (heretter **«** -systemansvarlig»), uten at dette berører anvendelsen av nasjonal lovgivning i hver europeisk juridisk enhet og autonomien og uavhengigheten til de europeiske selskapene som har etablert et lokalt styringssystem og

har en lokal systemansvarlig, som beskrevet i **vedlegg I,** og utveksling av informasjon mellom de ulike systemforvalterne, hvis det er aktuelt, som vil være tillatt for å sikre tilstrekkelig koordinering og bedre utførelse av deres oppgaver.

Styret, som er ansvarlig for implementeringen og utpeking av den fysiske personen som skal ha ansvaret for administrasjonen av systemet, har utnevnt stillingen som Head of Legal & Compliance i MIB Midea EU & Teka EU, og som stedfortreder stillingen Senior Compliance Specialist i MIB Midea EU & Teka EU. Den ansvarlige for systemet har delegert forvaltningen av meldinger mottatt gjennom den interne europeiske informasjonskanalen (i henhold til **vedlegg I,** som oppdateres jevnlig) til den lokale ansvarlige for systemet i Europa.

Formålet med denne policyen er å forklare den interne prosedyren for håndtering av den europeiske varslingskanalen, beskyttelse av varsleren og anvendelse av de generelle handlingsprinsippene, uten at dette berører endringer eller tilpasninger som er nødvendige for å overholde lokale forskrifter som gjelder for selskaper i Europa.

Dersom lokale forskrifter er i strid med prinsippene i denne policyen, vil alltid de lokale forskriftene som gjelder i hvert enkelt tilfelle ha forrang.

2. Hvem kan rapportere via den interne europeiske informasjonskanalen?

Personer som har eller har fått informasjon om brudd i en arbeids- eller yrkessammenheng i Den europeiske union (heretter «varsleren») kan sende inn varsler gjennom den interne europeiske varslingskanalen, herunder i alle tilfeller:

- Ansatte.

- Informanter som kommuniserer eller avslører informasjon om brudd som er innhentet i forbindelse med et arbeidsforhold eller et statutært forhold som er avsluttet: frivillige, stipendiater, praktikanter, uavhengig av om de mottar lønn eller ikke, samt de som ennå ikke har påbegynt et arbeidsforhold, når informasjonen om bruddene er innhentet under utvelgelsesprosessen eller forhandlingene før kontraktsinngåelsen.

- Aksjonærer, deltakere og personer som tilhører administrasjons-, ledelses- eller tilsynsorganet i selskapene i den europeiske gruppen, inkludert ikke-utøvende medlemmer.

- Tredjeparter som selskapene har en forretningsforbindelse med, enten det er kunder, leverandører, agenter, distributører, selvstendig næringsdrivende, entreprenører, underleverandører – og de som arbeider under tilsyn av disse – eller offentlige ansatte.

3. Hvordan får man tilgang til den interne europeiske informasjonskanalen?

I Europa finnes det en varslingskanal uten at dette berører lokale varslingskanaler (**vedlegg I**), på:

- **Nettplattform: https://whistleblowersoftware.com/secure/MideaEurope**

  Denne plattformen gjør det mulig å kommunisere skriftlig eller muntlig. Kommunikasjonen kan være anonym, hvis informanten ønsker det, og kan foregå på hvilket som helst språk, og konfidensialiteten til all kommunikasjon er garantert. Plattformen gjør det også mulig å angi hvilket selskap informanten ønsker å rapportere om.

- **Møte** med den ansvarlige for systemet innen maksimalt 7 dager etter forespørselen, med garanti for konfidensialitet.

I tillegg er det i virksomheter med mer enn 50 ansatte **lokale kanaler for å melde fra** tilgjengelig for informanten, som beskrevet i **vedlegg I**.

Uten at dette berører informantens rett til å velge det kommunikasjonsmiddelet han eller hun foretrekker, garanterer den interne europeiske informasjonskanalen autonomi, konfidensialitet, uavhengighet og fravær av interessekonflikter på grunn av sin uavhengighet fra kommersielle aktiviteter og lokale ansatte, siden den administreres av den europeiske compliance-funksjonen.

I samsvar med gjeldende lokale forskrifter kan det også finnes **eksterne klagekanaler** til de kompetente myndighetene og, hvis aktuelt, til institusjoner, organer eller organer i Den europeiske union (heretter **«uavhengig klageinstans»** eller «AAI»). Informanten vil bli informert av den ansvarlige for systemet om eksterne kommunikasjonskanaler og tilgangskrav som kan være fastsatt i de enkelte land.

4. Hva kan jeg kommunisere gjennom den interne europeiske informasjonskanalen?

Den interne europeiske informasjonskanalen tillater kommunikasjon av følgende:

i) **Brudd på eksterne regelverk**: slike meldinger kan omfatte ulovlige handlinger: svindel, korrupsjon, trakassering, utlevering av konfidensiell informasjon, skade på datasystemer, brudd på personvernet og personopplysninger, immaterielle rettigheter, skade på miljøet, brudd på menneskerettigheter eller arbeidstakerrettigheter osv.

ii) **Brudd på Midea-konsernets interne regelverk**: Slike meldinger kan omfatte handlinger som er i strid med Mideas **forretningsetiske retningslinjer** eller andre **interne** retningslinjer og prosedyrer **i** Midea-konsernet.

iii) **Spørsmål eller henvendelser** knyttet til tolkningen av konsernets retningslinjer eller etiske eller atferdsmessige spørsmål.

5. Hva er omfanget av beskyttelsen av varsleren i henhold til direktivet?

Tiltakene for beskyttelse av varsleren, som er fastsatt i punkt 8, gjelder varsleren og, i givet fall, de lovlige representantene for arbeidstakerne i utøvelsen av deres funksjoner som rådgivere og støttespillere for varsleren, samt: a) fysiske personer som, innenfor rammen av organisasjonen der varsleren arbeider, samarbeider i prosessen; b) fysiske personer som er knyttet til varsleren og som kan bli utsatt for represalier, for eksempel kolleger eller familiemedlemmer; c) juridiske personer som varsleren arbeider for eller har et arbeidsforhold til eller en betydelig eierandel i.

Overtredelser som er underlagt informantbeskyttelse, vil være de som fastsettes av hvert enkelt land ved gjennomføringen av direktivet, med skille mellom:

5.1 EUs beskyttelsesområde:

- **Handlinger eller unnlatelser som kan utgjøre brudd på EU-retten,** forutsatt at i) de faller innenfor anvendelsesområdet som er oppført i vedlegget til direktiv 2019/1937 av 23. oktober 2019; ii) de berører EUs interesser i henhold til artikkel 325 i traktaten om Den europeiske unions funksjon; eller iii) har innvirkning på det indre marked i henhold til artikkel 26.2 i traktaten om Den europeiske unions funksjon, herunder brudd på konkurransereglene og statsstøtte, samt brudd på skatteregler eller -praksis for selskaper med sikte på å oppnå en skattefordel som forvrenger formålet med eller virkningen av selskapsbeskatningslovgivningen.

5.2 Spansk beskyttelsesområde:

- Handlinger eller unnlatelser som kan utgjøre en **straffbar handling**.
- Handlinger eller unnlatelser som kan utgjøre en alvorlig eller svært alvorlig **administrativ overtredelse**.

5.3 Lokalt beskyttelsesområde:

Som nevnt kan lokale forskrifter i hvert europeisk land, på tidspunktet for gjennomføringen av direktivet, fastsette andre brudd som kan være omfattet av beskyttelsen av varsleren.

6. Forvaltning av den interne europeiske informasjonskanalen

i. Den interne europeiske informasjonskanalen tillater **skriftlig** eller **muntlig** kommunikasjon, eller begge deler. Informasjonen kan sendes skriftlig via nettplattformen og e-post, eller per telefon via de kanalene som er angitt i punkt 3 ovenfor. På forespørsel fra varsleren kan informasjonen også gis ved et møte med den ansvarlige for systemet innen syv (7) dager fra forespørselen.

ii. **Muntlig kommunikasjon** skal dokumenteres, med informantens samtykke: i) ved hjelp av en opptak eller ii) en fullstendig og nøyaktig transkripsjon av samtalen, og

informanten skal gis mulighet til å kontrollere, korrigere og godta transkripsjonen ved å signere den.

iii. Det europeiske interne informasjonskanalen tilbyr muligheten til å sende inn **anonyme** meldinger via nettplattformen.

iv. Når informanten sender en melding, kan han eller hun oppgi en adresse, e-postadresse eller et sikkert sted for å motta eller fravelge **varsler** om statusen på meldingen.

v. Når en melding sendes via den interne europeiske informasjonskanalen, vil det innen syv (7) kalenderdager bli sendt en **bekreftelse** på mottakelsen, med mindre dette kan sette konfidensialiteten av meldingen i fare.

vi. Den ansvarlige for systemet vil informere informanten, den berørte personen og vitnene om behandlingen av deres data i henhold til vilkårene fastsatt i direktivet.

vii. Når meldingen sendes via nettstedet, vil det på forespørsel fra informanten genereres et **tilgangsnummer og et passord**, som informanten kan bruke til å følge opp meldingen sin.

viii. Den ansvarlige for systemet skal informere informanten om resultatet av undersøkelsen **innen tre (3) måneder** fra mottakelsen av meldingen eller tre (3) måneder fra utløpet av fristen på syv dager etter at meldingen ble sendt, med unntak av særlig komplekse saker som krever en forlengelse av fristen, i hvilket tilfelle fristen kan forlenges med inntil tre (3) måneder.

ix. Systemansvarlig kan **kommunisere** med informanten og be om ytterligere informasjon.

x. Systemansvarlig kan også få **støtte og samarbeid fra andre områder** av konsernet eller selskapet eller fra eksterne rådgivere, når det er nødvendig, i forbindelse med undersøkelsen.

xi. **Den berørte personen** vil bli informert om anmeldelsen av handlingene eller unnlatelsene som tilskrives ham eller henne, samt om hans eller hennes rett til å bli hørt, på det tidspunktet og på den måten som den ansvarlige for den interne europeiske informasjonskanalen anser hensiktsmessig for å sikre et godt resultat av undersøkelsen.

xii. Retten til **uskyldspresumpsjon og æren** til de personene som berøres av kommunikasjonen, skal respekteres.

xiii. De berørte personene skal også nyte samme beskyttelse som informantene, ved at deres identitet holdes hemmelig og det sikres konfidensialitet rundt fakta og beskyttelse av personopplysninger.

xiv. Hvis de rapporterte fakta faller innenfor ansvarsområdet til den ansvarlige for systemet, eller på noen måte kan skape en **interessekonflikt** for noen av personene som er involvert i behandlingen og/eller etterforskningen av meldingen, skal den berørte personen avstå fra å delta i behandlingen av meldingen.

xv. Systemansvarlig kan **nekte å ta imot en melding** når de rapporterte fakta blant annet mangler troverdighet og grunnlag.

xvi. Håndteringssystemet for den interne europeiske informasjonskanalen er utformet og etablert for **sikker håndtering** i samsvar med personvernregelverket.

xvii. Den interne europeiske informasjonskanalen garanterer **konfidensialiteten** til informantens identitet og enhver tredjepart som er nevnt i meldingen, **og hindrer uautorisert personell i å få tilgang til den**. Informanten vil under ingen omstendigheter få tilgang til meldingen, med unntak av når det kreves av , domstolen, påtalemyndigheten eller den kompetente administrative myndigheten i forbindelse med en strafferettslig, disiplinær eller sanksjonell etterforskning.

xviii. Den ansvarlige for systemet har en **prosedyre for håndtering av meldinger mottatt** gjennom den interne europeiske informasjonskanalen som utfyller denne policyen.

7. Ingen represalier

Konsernet vil sørge for at det ikke forekommer handlinger som utgjør represalier, inkludert trusler om represalier og forsøk på represalier mot personer som sender inn en melding gjennom den interne europeiske informasjonskanalen.

Med gjengjeldelse menes enhver handling eller unnlatelse som direkte eller indirekte innebærer en ugunstig behandling som setter personene som utsettes for den i en særlig ugunstig situasjon i forhold til andre i arbeids- eller yrkessammenheng, utelukkende på grunn av deres status som informanter eller fordi de har gjort en offentlig avsløring, forutsatt at slike handlinger eller unnlatelser finner sted under etterforskningsprosedyren eller i løpet av de to årene etter at etterforskningen er avsluttet.

Som eksempel kan nevnes represalier som, på grunn av deres status som varslere, tar form av:

- Suspensjon av arbeidsavtalen, oppsigelse, opphør av arbeidsforholdet eller statutten, inkludert manglende fornyelse eller tidlig oppsigelse av en midlertidig arbeidsavtale etter prøveperioden, eller tidlig oppsigelse eller annullering av kontrakter om varer eller tjenester, pålegg av disiplinærtiltak, degradering eller nektelse av forfremmelse og enhver annen vesentlig endring av arbeidsvilkårene. manglende omgjøring av en midlertidig arbeidsavtale til en tidsubegrenset avtale, når arbeidstakeren hadde en berettiget forventning om å bli tilbudt en fast stilling; med mindre disse tiltakene gjennomføres som ledd i den ordinære utøvelsen av ledelsesmyndigheten som er fastsatt i arbeidslovgivningen eller i de relevante forskriftene for offentlig tjeneste, på grunn av påviste omstendigheter, forhold eller overtredelser, og uten sammenheng med innleveringen av meldingen til den europeiske interne informasjonskanalen.
- Skader og tap, herunder skade på omdømme, økonomiske tap, tvang, trusler, trakassering eller utstøting.
- Negativ vurdering eller referanser om arbeids- eller yrkesutførelsen utelukkende på grunn av deres status som varslere.
- Oppføring på svartelister eller spredning av informasjon i en bestemt sektor, som vanskeliggjør eller hindrer tilgang til arbeid eller oppdrag eller tjenester.
- Nektelse eller kansellering av lisens eller tillatelse.
- Nektelse av opplæring.
- Diskriminering eller ugunstig eller urettferdig behandling.

Hvis konsernet får kjennskap til at det foregår eller har foregått represalier, vil det treffe rimelige tiltak for å stoppe og håndtere dem. Disse tiltakene kan, etter behov, bestå i:

- Å gjeninnsette personen i samme stilling eller en tilsvarende stilling, med samme lønn, ansvar, stilling og omdømme.
- Gi likeverdig tilgang til forsvar, opplæring, muligheter, fordeler og rettigheter.
- Gjeninnsette personen i sin tidligere stilling i organisasjonen

- Å avslutte eller trekke tilbake eventuelle konflikter eller tvister som måtte eksistere mot personen (for eksempel holdning eller behandling);
- Be om unnskyldning for eventuelle skader som er påført;

8. Beskyttelsestiltak overfor den uavhengige myndigheten for beskyttelse av varslere.

Informanter som rapporterer brudd på punkt 5.1, 5.2 og 5.3, har rett til beskyttelsestiltak fra den uavhengige myndigheten for beskyttelse av informanter (**,** heretter **«AAI»),** som hvert europeisk land har opprettet, når det er relevant, under følgende omstendigheter:

- Det foreligger rimelig grunn til å tro at informasjonen som det refereres til, er sann på tidspunktet for meldingen, selv om det ikke foreligger avgjørende bevis, og at informasjonen faller innenfor virkeområdet til punkt 5.1, 5.2 og 5.3.
- Meldingen eller offentliggjøringen er gjort i samsvar med kravene i direktivet eller andre gjeldende lokale forskrifter.

Personer som kommuniserer eller videreformidler:

i. Informasjon som er inneholdt i meldinger som har vært uakseptable.
ii. Informasjon relatert til klager om mellommenneskelige konflikter eller som kun berører informanten og personene som er omfattet av kommunikasjonen eller avsløringen.
iii. Informasjon som allerede er offentlig kjent eller som kun utgjør rykter.
iv. Informasjon som refererer til handlinger eller unnlatelser som ikke er omfattet av virkeområdet til punkt 5.1, 5.2 og 5.3 i denne policyen.

Alt dette uten at det berører tilleggsvilkår og unntak som kan være fastsatt i andre lokale forskrifter som kan være gjeldende.

Støttetiltakene fra den uavhengige myndigheten for beskyttelse av varslere kan, avhengig av regelverket i hvert land, bestå av å tilby følgende, avhengig av tilfellet:

i. Utfyllende, uavhengig og gratis informasjon og rådgivning om tilgjengelige prosedyrer og ressurser, beskyttelse mot represalier og rettighetene til den berørte personen.
ii. Effektiv bistand for beskyttelse mot represalier.
iii. Juridisk bistand i straffesaker og i sivile saker på tvers av landegrensene, i samsvar med gjeldende lovgivning og EU-regelverk.
iv. Finansiell og psykologisk støtte, i unntakstilfeller, etter vurdering av det uavhengige klageorganet i hvert land.

Alt dette uten at det berører retten til gratis juridisk bistand for representasjon og forsvar i rettssaker, som også kan gis i henhold til hvert lands regelverk.

Den ansvarlige for systemet skal gi informanten informasjon om støttetiltakene som tilbys av lokale AAI-er.

9. Databeskyttelse og konfidensialitet

Behandlingen av personopplysninger i det europeiske interne informasjonskanalen vil skje i samsvar med kravene fastsatt i forordning (EU) 2016/679 av Europaparlamentet og rådet av 27. april 2016 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger og om oppheving av direktiv 95/46/ (heretter **«GDPR»),** samt den spanske loven 3/2018 av 5. desember om beskyttelse av personopplysninger og garanti for digitale rettigheter (heretter **«LOPDGDD»)**. I denne sammenheng er TEKA INDUSTRIAL S.A., med NIF- A-39004932 og hovedkontor i Calle Cajo 17, 39011 Santander, Spania, ansvarlig for behandlingen.

9.1. Begrensning av formålet

Personopplysninger som samles inn gjennom den interne europeiske informasjonskanalen, vil bli behandlet utelukkende med det formål å behandle mottatte meldinger og undersøke de anmeldte hendelsene.

9.2. Legitimering av behandlingen

Behandlingen av personopplysninger, med det formål å kunne behandle meldinger mottatt gjennom den interne europeiske informasjonskanalen, er lovlig og har sin rettslig grunnlag i oppfyllelsen av en lov forpliktelse, i samsvar med bestemmelsene i artikkel 30.2 i lov 2/2023.

Behandlingen av ikke-obligatoriske opplysninger, samt behandlingen av personopplysninger som følge av offentliggjøring, vil være basert på allmennhetens interesse som fastsatt i GDPR, i samsvar med bestemmelsene i artikkel 6.1.e) i GDPR.

Behandling av spesielle kategorier av personopplysninger av hensyn til viktige allmenne interesser kan utføres i samsvar med artikkel 9.2.g) i GDPR.

9.3. Begrensning av tilgang til data:

Tilgang til personopplysninger i det interne europeiske informasjonskanalen vil være begrenset til: i) den som er ansvarlig for systemet og som direkte administrerer de lokale klagekanalene; ii) personalavdelingen, når det er hensiktsmessig å iverksette disiplinærtiltak; iii) konsernets etikkontor, når det er nødvendig å involvere seg i etterforskningen og/eller hensiktsmessig å iverksette rettslige eller disiplinærtiltak; iv) de som er ansvarlige for databehandlingen, og v) personvernombudet, hvis dette er obligatorisk, og vi) enhver annen person som må ha tilgang av behørig begrunnet årsaker.

I tillegg kan personopplysninger deles med andre enheter i Midea-konsernet for å koordinere, administrere og, om nødvendig, gjennomføre de tiltak og/eller tiltak som er nødvendige for å administrere og behandle meldingen og, om nødvendig, den åpne etterforskningen i hvert enkelt tilfelle.

Personopplysninger (inkludert spesielle kategorier av personopplysninger) kan overføres og lagres i et mottakerland utenfor Det europeiske økonomiske samarbeidsområdet («EØS»). De kan også behandles av morselskapet og datterselskapene utenfor EØS. Når selskapet overfører personopplysninger utenfor EØS, vil det sikre at alle nødvendige garantier for å beskytte personopplysningene med samme beskyttelse som de gis innenfor EØS, og at overføringen er i samsvar med personvernforordningen og alle andre gjeldende forskrifter. Dette kan oppnås på flere måter, blant annet:

- Mottakerlandet som dataene sendes til, kan være godkjent av EU-kommisjonen for å tilby et tilstrekkelig beskyttelsesnivå, eller
- Mottakeren har inngått en avtale basert på «standardkontraktsklausuler» godkjent av EU-kommisjonen, som forplikter mottakeren til å beskytte personopplysningene på samme måte som de beskyttes innenfor EØS.

I andre tilfeller kan loven tillate overføring av den ansattes personopplysninger utenfor EØS på annen måte. I alle tilfeller vil selskapet imidlertid sørge for at enhver overføring av personopplysninger er i samsvar med personvernlovgivningen.

For mer informasjon om beskyttelsen av personopplysninger når de overføres utenfor EØS, kan du kontakte dataprotection@teka.com

Overføring av data er beskyttet av selskapets berettigede interesse i å behandle kommunikasjonen på riktig måte, i samsvar med betraktning 48 i GDPR. Utelukkende i tilfelle det oppdages en ulovlig handling, kan personopplysninger bli videreformidlet til tredjeparter (domstoler, politimyndigheter eller offentlige myndigheter) for å oppfylle de relevante lovmessige forpliktelsene.

9.4 Oppbevaringstid for data

Opplysningene som behandles i den interne europeiske informasjonskanalen, kan kun oppbevares i denne så lenge det er nødvendig for å avgjøre om det er hensiktsmessig å iverksette en intern undersøkelse.

I alle tilfeller vil opplysningene bli slettet tre måneder etter mottakelsen av meldingen, med mindre formålet med oppbevaringen er å dokumentere kanalens funksjon eller det kan utgjøre en straffbar handling, i hvilket tilfelle opplysningene vil bli oppbevart så lenge det er nødvendig under rettsprosessen.

9.5. Utøvelse av rettigheter

Personer hvis personopplysninger behandles i rammen og konteksten av den interne europeiske informasjonskanalen, vil bli informert om behandlingen av deres personopplysninger, i henhold til vilkårene i artikkel 13 og 14 i GDPR.

De kan utøve sine rettigheter til innsyn, retting, sletting, innsigelse, begrensning og portabilitet som er anerkjent i artikkel 15 til 22 i GDPR, ved å sende en skriftlig henvendelse til e-postadressen:dataprotection@teka.com eller til den spanske datatilsynsmyndigheten (www.aepd.es). Når den interesserte utøver retten til innsigelse, vil det imidlertid antas at det, med mindre det foreligger bevis for det motsatte, foreligger tvingende legitime grunner som rettferdiggjør behandlingen av personopplysningene, og denne retten vil derfor ikke være effektiv.

Retten til innsyn i personopplysninger omfatter under ingen omstendigheter identiteten til informanten, og muligheten til å kommunisere denne identiteten er begrenset til kun å gjelde rettsmyndigheter, påtalemyndigheten eller den kompetente administrative myndigheten i forbindelse med en strafferettslig, disiplinær eller sanksjonell etterforskning.

9.6. Prinsippet om proporsjonalitet og minimering av data

Det vil kun bli samlet inn personopplysninger som er relevante. Hvis det ikke er relevant for behandlingen av spesifikk informasjon, eller hvis de blir samlet inn ved et uhell, vil de bli slettet uten unødig forsinkelse. Likeledes vil alle personopplysninger som er blitt kommunisert og som refererer til atferd som ikke faller innenfor virkeområdet for denne policyen, bli slettet. Hvis den mottatte informasjonen inneholder personopplysninger som faller innenfor spesielle kategorier av opplysninger, vil disse bli slettet umiddelbart, uten at de blir registrert eller behandlet.

9.7 Sikkerhetstiltak:

Den interne europeiske informasjonskanalen er utformet, etablert og administrert på en sikker måte, slik at den garanterer konfidensialiteten til identiteten til informanten og eventuelle tredjeparter som er nevnt i meldingen, samt til handlingene som utføres i

forbindelse med håndteringen og behandlingen av meldingen, og hindrer tilgang for uautorisert personell.

Dermed har den interne europeiske informasjonskanalen tekniske og organisatoriske tiltak for å ivareta sikkerheten til de innsamlede dataene og konfidensialiteten til meldingene, med det formål å beskytte dem mot urettmessig spredning og tilgang.

10. Bruk av den interne europeiske informasjonskanalen og politikken

Bruk av den europeiske interne informasjonskanalen og politikken som utvikler den, skal skje i god tro, og det vil ikke anses å være i samsvar med prinsippet om god tro eller formålet med retningslinjene og gjeldende regelverk som utvikler beskyttelsen av personer som rapporterer brudd på regelverket og antikorrupsjon, å fremlegge falsk, ubegrunnet, forvrengt informasjon, samt informasjon som er innhentet ulovlig for å skade og skade personer eller selskaper i konsernet.

11. Brudd

Alle personer som er omfattet av denne policyen, er forpliktet til å overholde innholdet i den. Dersom det oppdages et alvorlig brudd på denne policyen eller andre elementer i den interne europeiske informasjonskanalen, kan og skal dette meldes til systemansvarlig.

12. Endringer

Denne policyen vil bli gjennomgått og oppdatert årlig, med mindre det er nødvendig å gjøre det på et tidligere tidspunkt, uten at dette berører systemansvarliges rett til å foreta nødvendige korreksjoner, rettelser eller avklaringer.

Denne policyen erstatter alle tidligere policyer for varsling som er godkjent av styret i Teka Industrial, S.A.

13. Juridisk karakter

Politikk for den interne europeiske informasjonskanalen Midea & Teka Europe

Denne policyen er i samsvar med direktiv (EU) 2019/1937 fra Europaparlamentet og rådet av 23. oktober 2019 om beskyttelse av personer som varsler om brudd på EU-retten og rådsretten, og kravene i lov 2/2023 om beskyttelse av personer som varsler om brudd på regelverket og antikorrupsjon.

Alt dette uten at det berører øvrige europeiske forskrifter som gjennomfører dette direktivet, og som skal overholdes og gjelde for forvaltning og beskyttelse dersom det ikke er uttrykkelig nevnt i denne policyen.

Vedlegg I – Lokalt klagekanal

Zepa SpA	mippolito@carnelutti.com
Midea Italia S.r.l	https://mis.integrityline.com/
Teka Portugal SA	Speak-up@teka.pt

Vedlegg II: Enheter som omfattes av denne policyens virkeområde

Teka Industrial, S.A.
Steelgran Components, S.A
Sitre telecom, S.A
Küppersbusch Hausgeräte GMBH
Teka Austria GmbH
Teka CZ SRO
Teka Bulgaria EOOD
Teka Polska Sp Zo.o
SC Teka Küchentechnik Romania Srl
Teka France SAS
Teka Portugal SA
Teka Hellas AE
Zepa SpA
Intra Holding AS
Intra AS
Intra Mölntrop AB
Juvel AS

Politikk for den interne europeiske informasjonskanalen Midea & Teka Europe

Midea Europe GmbH
Midea Electric France SAS
Midea Italia Srl
Midea Homeappliances UK Ltd