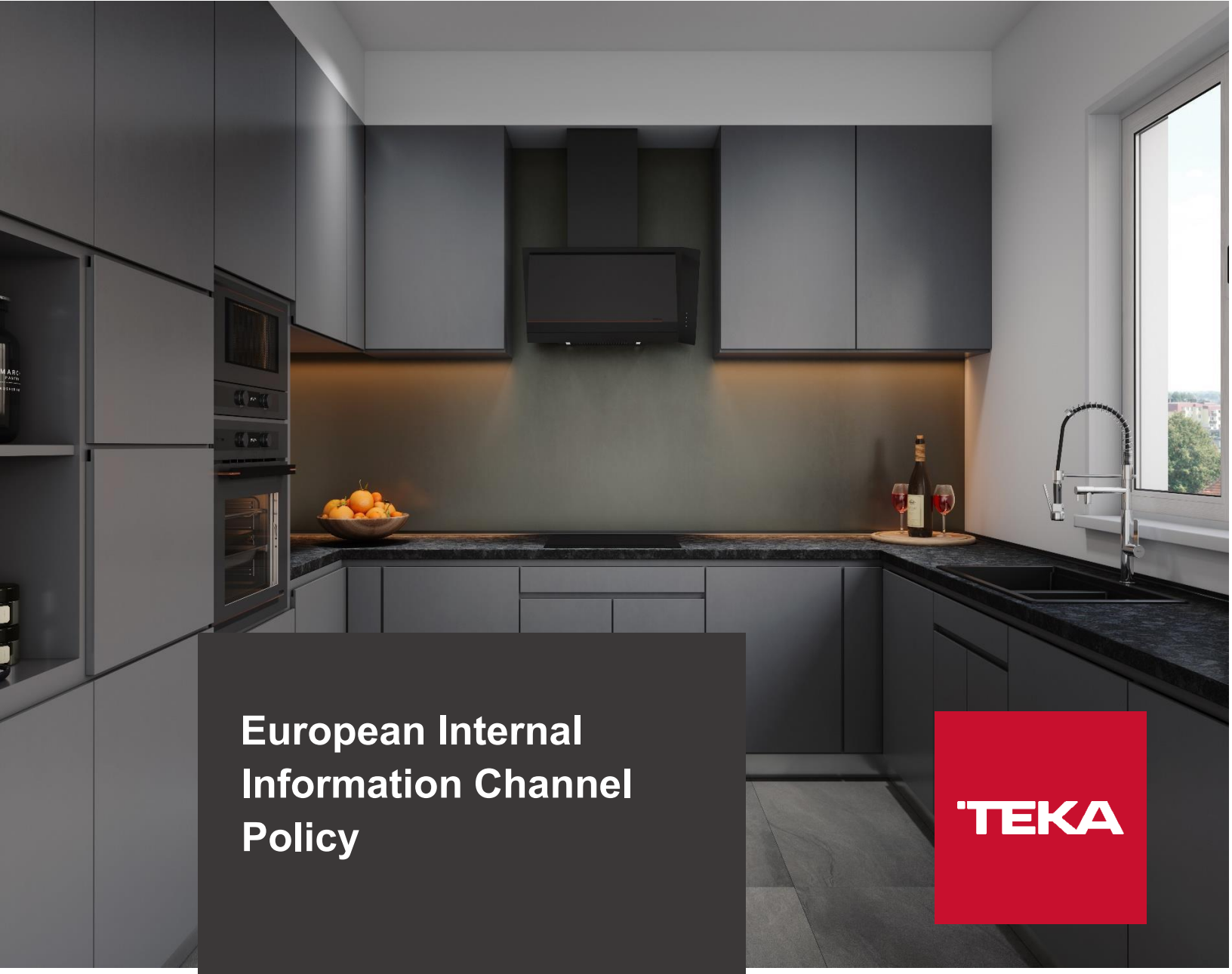

European Internal Information Channel Policy

Approved by the Board of Directors of
TEKA INDUSTRIAL, S.A.

European Internal Information Channel Policy Midea & Teka Europe

1. Introduction and purpose

Teka Industrial, S.A., its subsidiaries and the European entities of Midea's home appliance division are part of Midea Group Co. Ltd. ("Midea Group"). Midea Group is committed to conducting its business in all regions with integrity and in compliance with the law.

In the European region, an Internal Reporting Channel has been implemented in accordance with the requirements of Law 2/2023 of 20 February, regulating the protection of persons reporting regulatory infringements and combating corruption, which transposes Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (hereinafter, the **"Directive**"), as well as Regulation (EU) 2016/679 and Organic Law 3/2018 on the protection of personal data and the guarantee of digital rights. The European Internal Reporting Channel integrates all reporting channels in Europe and its scope of application includes Teka Industrial, S.A., all its subsidiaries in Europe and Midea's household appliance entities in Europe and the United Kingdom, as detailed **in Annex II.**

The purpose of this Policy is to provide a reporting channel available to the European Union (including the United Kingdom) (hereinafter, "the **European Internal Reporting Channel**") and is designed, established and managed in such a way as to allow: i) its accessible use; ii) the submission of written and/or verbal communications; (iii) respect for confidentiality and anonymity guarantees, except in cases where disclosure is required by national law or requested in the context of legal proceedings; (iv) protection against retaliation; (v) effective management of communications and appropriate follow-up; (vi) integration of the various reporting channels in Europe (including the United Kingdom); and (vii) protection of personal data.

The European Internal Information Channel is intended for employees and third parties of all companies listed in **Annex II** and is managed by Teka Industrial, S.A. of Spain with the support of the System Manager (hereinafter, the " **System Manager**"), without prejudice to the application in each European legal entity of the respective national legislation and the autonomy and independence of those European companies that have established a local governance system and have a local system manager, as detailed in

Annex I, and the exchange of information between the different system managers, if any, which shall be admissible for the proper coordination and better performance of their functions.

The Board of Directors, as the body responsible for implementation and for appointing the individual responsible for managing the system, has appointed the Head of Legal & Compliance at MIB Midea EU & Teka EU, and as deputy, the Senior Compliance Specialist at MIB Midea EU & Teka EU. The person responsible for the system has delegated the management of communications received through the European Internal Information Channel (as per **Annex I,** which is updated periodically) to the local person responsible for the system in Europe.

The purpose of this Policy is to explain the internal procedure for managing the European reporting channel, protecting whistleblowers and applying general principles of action, without prejudice to any modifications or adaptations that may be necessary to comply with local regulations applicable to companies in Europe.

In the event of a conflict between local regulations and the principles of this Policy, the local regulations applicable in each specific case shall always prevail.

2. Who can report through the European Internal Information Channel?

Individuals who have or have obtained information about infringements in a work or professional context in the European Union (hereinafter, the "Whistleblower") may submit reports through the European Internal Reporting Channel, including in any case:

- Employees.
- Whistleblowers who communicate or disclose information about breaches obtained in the context of a terminated employment or statutory relationship: volunteers, interns, trainees, regardless of whether they receive remuneration, as well as those whose employment relationship has not yet begun, when the information about the breaches was obtained during the selection process or pre-contractual negotiations.

- Shareholders, participants and persons belonging to the administrative, management or supervisory body of the companies of the European group, including non-executive members.

- Third parties with whom the companies have a business relationship, whether they are customers, suppliers, agents, distributors, self-employed persons, contractors, subcontractors —and those working under their supervision— or public employees.

3. How to access the European Internal Reporting Channel?

In Europe, a reporting channel is available without prejudice to local reporting channels (**Annex I**) at:

- **Web platform:** https://whistleblowersoftware.com/secure/MideaEurope

  This platform allows communications to be made in writing or verbally. Communications can be submitted anonymously, if the Whistleblower so chooses, and in any language, guaranteeing the confidentiality of all communications. The web platform also allows the company about which the Whistleblower wishes to report to be indicated.

- **Meeting** with the person responsible for the system within a maximum of 7 days of the request and guaranteeing confidentiality.

In addition, in entities with more than 50 employees, **local reporting channels** are made available to the Whistleblower, as detailed in **Annex I**.

Without prejudice to the Whistleblower's right to choose their preferred means of communication, the European Internal Reporting Channel guarantees autonomy, confidentiality, independence and the absence of conflicts of interest due to its disconnection from commercial activities and local employees, as it is managed by the European Compliance Function.

In accordance with applicable local regulations, there may also be **External Reporting Channels** to the competent authorities and, where applicable, to the institutions, bodies or agencies of the European Union (hereinafter, the **"Independent Whistleblower Protection Authority"** or "IAP"). The Whistleblower will be informed by the system manager about the external communication channels and access requirements that may be established in each country.

4. What can I report through the European Internal Reporting Channel?

The European Internal Reporting Channel allows for the reporting of any:

i) **Violations of external regulations**: these communications may include acts contrary to the law: fraud, corruption, harassment, disclosure of confidential information, damage to computer systems, violation of privacy and personal data, intellectual property rights, damage to the environment, violations of human or labour rights, etc.

ii) **Breaches of Midea Group internal regulations**: these reports may include acts contrary to Midea's **Code of Business Conduct** or other Midea **Group internal** policies and procedures.

iii) **Questions or queries** related to the interpretation of Group policies or ethical or behavioural issues.

5. What is the scope of protection for whistleblowers under the Directive?

The whistleblower protection measures set out in section 8 shall apply to the whistleblower and, where applicable, to the legal representatives of employees in the exercise of their duties of advising and supporting the whistleblower, as well as: a) natural persons who, within the framework of the organisation in which the whistleblower provides services, collaborate in the process; b) natural persons who are related to the whistleblower and who may suffer retaliation, such as co-workers or family members; c) legal persons for whom

the whistleblower works or with whom they have an employment relationship or a significant interest.

The offences subject to whistleblower protection will be those established by each country at the time of transposition of the Directive, distinguishing between:

5.1 Scope of protection of the European Union:

- **Acts or omissions that may constitute infringements of European Union law,** provided that (i) they fall within the scope listed in the Annex to Directive 2019/1937 of 23 October 2019; (ii) they affect the interests of the European Union within the meaning of Article 325 of the Treaty on the Functioning of the European Union; or (iii) have an impact on the internal market within the meaning of Article 26(2) of the Treaty on the Functioning of the European Union, including infringements of competition and State aid rules, and infringements of corporate tax rules or practices aimed at obtaining a tax advantage that distorts the object or purpose of the applicable corporate tax legislation.

5.2 Scope of Spanish protection:

- Actions or omissions that may constitute a **criminal offence**.
- Actions or omissions that may constitute a serious or very serious **administrative offence**.

5.3 Local scope of protection:

As indicated, the local regulations of each European country may provide, at the time of transposition of the Directive, for other infringements that may be subject to whistleblower protection.

6. Management of the European Internal Information Channel

i. The European Internal Information Channel allows communications to be made in **writing**, **verbally** or by both means. Information may be submitted in writing, via

the web platform and email, or by telephone through the channels enabled and detailed in section 3 above. At the request of the Whistleblower, it may also be submitted through a meeting with the person responsible for the system within seven (7) days of the request.

ii. **Verbal communications** will be documented, with the consent of the Whistleblower: i) by means of a recording or ii) a complete and accurate transcript of the conversation, and the Whistleblower will be given the opportunity to verify, rectify and accept the transcript by signing it.

iii. The European Internal Reporting Channel offers the possibility of submitting **anonymous** communications via the web platform.

iv. When submitting a communication, the Whistleblower may indicate an address, email address or secure location for the purpose of receiving **notifications** about the status of their communication or opting out of them.

v. The submission of a report through the European Internal Information Channel will result in the receipt of an **acknowledgement of receipt** within a maximum of seven (7) calendar days, confirming receipt of the report, unless this could jeopardise its confidentiality.

vi. The person responsible for the system will inform the Whistleblower, the person concerned and any witnesses of the processing of their data in accordance with the terms of the Directive.

vii. When the communication is sent via the website, an **access number and password** will be generated at the request of the Whistleblower, through which they will be able to track their communication.

viii. The System Manager shall inform the Whistleblower of the outcome of the investigation within a period not **exceeding three (3) months** from receipt of the communication or three (3) months from the expiry of the seven-day period after the communication was made, except in cases of particular complexity requiring an extension of the period, in which case it may be extended for a maximum of three (3) additional months.

ix. The System Manager may **communicate** with the Whistleblower and request additional information.

x. Likewise, the System Manager may seek the **support and collaboration of other areas** of the Group or the company or external advisors, when necessary, within the framework of the investigation.

xi. **The person concerned** will be informed of the allegations of acts or omissions attributed to them, as well as their right to be heard, at the time and in the manner deemed appropriate by the European Internal Information Channel Manager to ensure the successful outcome of the investigation.

xii. The right to the **presumption of innocence and to the honour** of the persons affected by the communication shall be respected.

xiii. Likewise, the persons concerned shall enjoy the same protection as that established for whistleblowers, with their identity being kept confidential and the confidentiality of the facts and the protection of personal data being guaranteed.

xiv. If the facts reported fall within the scope of the System Manager's duties or could in any way give rise to a **conflict of interest** for any of the persons involved in the process of managing and/or investigating the report, the person concerned shall refrain from participating in the process of handling the report.

xv. The System Manager may **refuse to accept a report** if the facts reported lack credibility and substance, among other reasons.

xvi. The European Internal Information Channel management system is designed and established for **secure management** and in compliance with data protection regulations.

xvii. The European Internal Information Channel guarantees the **confidentiality** of the identity of the Whistleblower and any third party mentioned in the communication, **preventing access by unauthorised personnel**. Under no circumstances will access be given to the communication submitted by the Whistleblower, except when required by the judicial authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or sanctioning investigation.

xviii. The person responsible for the system has a **procedure** in place **to manage communications received** through the European Internal Information Channel, which complements this Policy.

7. No retaliation

The Group shall ensure that no acts of retaliation, including threats of retaliation and attempts at retaliation, are taken against persons who submit a communication through the European Internal Information Channel.

Retaliation is understood to mean any act or omission that, directly or indirectly, involves unfavourable treatment that places the persons suffering it at a particular disadvantage in relation to others in the workplace or professional context, solely because of their status as Whistleblowers or because they have made a public disclosure, provided that such acts or omissions occur during the investigation procedure or within two years of the investigation's completion.

By way of example, retaliation is considered to be any action taken against a whistleblower in their capacity as such in the form of:

- Suspension of the employment contract, dismissal, termination of the employment or statutory relationship, including non-renewal or early termination of a temporary employment contract after the probationary period, or early termination or cancellation of contracts for goods or services, imposition of any disciplinary measure, demotion or denial of promotion, and any other substantial change in working conditions; failure to convert a temporary employment contract into a permanent one, where the worker had a legitimate expectation that he or she would be offered permanent employment; unless these measures are taken in the regular exercise of management powers provided for in labour legislation or in the relevant civil service regulations, due to proven circumstances, facts or infringements, and un ly related to the submission of the report to the European Internal Information Channel.
- Damages, including damage to reputation, financial loss, coercion, intimidation, harassment or ostracism.
- Negative evaluations or references regarding work or professional performance solely due to their status as Whistleblowers.

- Inclusion on blacklists or dissemination of information in a specific sector, which hinders or prevents access to employment or the contracting of works or services.
- Refusal or cancellation of a licence or permit.
- Denial of training.
- Discrimination or unfavourable or unfair treatment.

If the Group becomes aware that reprisals are taking place or have taken place, it will take reasonable measures to stop and address them. These measures, as appropriate, may consist of:

- Reinstating the person to the same or an equivalent position, with the same salary, responsibilities, title and reputation;
- Allowing equal access to defence, training, opportunities, benefits and rights.
- Reinstating the person to their previous professional position in relation to the organisation;
- Ending or withdrawing any conflict or litigation that may exist against the person (e.g., attitude or treatment offered);
- Apologise for any harm suffered;

8. Protective measures before the Independent Authority for the Protection of Whistleblowers.

Whistleblowers who report breaches of sections 5.1, 5.2 and 5.3 shall be entitled to protective measures before the Independent Authority for the Protection of Whistleblowers (hereinafter **"IAP"),** which each European country has established, where appropriate, when the following circumstances arise:

- There are reasonable grounds to believe that the information referred to is truthful at the time of communication, even if no conclusive evidence is provided, and that the information falls within the scope of sections 5.1, 5.2 and 5.3.
- The communication or disclosure has been made in accordance with the requirements of the Directive or other applicable local regulations.

Persons who communicate or disclose:

i. Information contained in communications that have been inadmissible.
ii. Information related to complaints about interpersonal conflicts or that only affect the Whistleblower and the persons referred to in the communication or disclosure.
iii. Information that is already in the public domain or constitutes mere rumours.
iv. Information referring to actions or omissions not included in the scope of sections 5.1, 5.2 and 5.3 of this Policy.

All of the above is without prejudice to any additional conditions and exclusions that may be provided for in other applicable local regulations.

The support measures provided by the Independent Authority for the Protection of Whistleblowers, depending on the regulations of each country, may consist, as appropriate, of providing:

i. Comprehensive, independent and free information and advice on the procedures and resources available, protection against retaliation and the rights of the person concerned.
ii. Effective assistance for protection against retaliation.
iii. Legal assistance in criminal proceedings and cross-border civil proceedings, in accordance with applicable Community legislation and regulations.
iv. Financial and psychological support, on an exceptional basis, following assessment by the AAI in each country.

All of this is without prejudice to the right to free legal aid for representation and defence in legal proceedings, which may also be granted under the regulations of each country.

The system manager shall provide the Whistleblower with information on the support measures offered by local AAIs.

9. Data protection and confidentiality

The processing of personal data by the European Internal Information Channel will be carried out in accordance with the requirements set out in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural

persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ EC (hereinafter, the **"GDPR"),** as well as Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights (hereinafter, the **"LOPDGDD")**. For these purposes, TEKA INDUSTRIAL S.A., with Tax Identification Number A-39004932 and registered office at Calle Cajo 17, 39011 Santander, Spain, is the entity responsible for processing.

9.1. Limitation of purpose

Personal data collected through the European Internal Information Channel will be processed for the sole purpose of processing the communications received and investigating the reported incidents.

9.2. Legitimacy of processing

The processing of personal data for the purpose of handling communications received through the European Internal Information Channel is lawful and has its basis in legitimacy in the fulfilment of a legal obligation, in accordance with the provisions of Article 30.2 of Law 2/2023.

The processing of non-mandatory data, as well as the processing of personal data resulting from public disclosure, will be based on the public interest provided for in the GDPR, in accordance with the provisions of Article 6.1.e) of the GDPR.

The processing of special categories of personal data for reasons of substantial public interest may be carried out in accordance with Article 9.2.g) of the GDPR.

9.3. Restriction of access to data:

Access to personal data contained in the European Internal Reporting Channel shall be limited to: i) the system manager and those who directly manage the local reporting channels; ii) the Human Resources department, when it is appropriate to take disciplinary measures; iii) the Group Ethics Office, when it is necessary to involve them in the investigation and/or appropriate to take legal or disciplinary measures; iv) data processors, and v) the data protection officer, if mandatory, and vi) any other person who needs access for duly justified reasons.

In addition, personal data may be shared with other entities of the Midea Group for the purpose of coordinating, managing and, where appropriate, executing the actions and/or measures necessary for the management and processing of the communication and, where appropriate, the investigation opened in each case.

Personal data (including special categories of personal data) may be transferred and stored in a destination country outside the European Economic Area ("EEA"). It may also be processed by the parent company and subsidiaries outside the EEA. When the company transfers personal data outside the EEA, it will ensure that all necessary safeguards are in place to protect personal data with the same protection as it is afforded within the EEA and that the transfer complies with the General Data Protection Regulation and all other applicable regulations. This can be achieved in several ways, including:

- The destination country to which the data is sent could be approved by the European Commission for offering an adequate level of protection; or
- The recipient has entered into a contract based on the 'standard contractual clauses' approved by the European Commission, which oblige them to protect your personal data in the same way as it is protected within the EEA.

In other circumstances, the law may allow the transfer of employee personal data outside the EEA in other ways. However, in all cases, the company will ensure that any transfer of personal data complies with data protection legislation.

For further details on the protection afforded to personal data when transferred outside the EEA, please contact dataprotection@teka.com

The communication of data is covered by the company's legitimate interest in correctly processing the communications made, in accordance with recital 48 of the GDPR. Only in the event of an illegal act being detected may personal data be communicated to third parties (courts and tribunals, law enforcement agencies or public authorities) in order to comply with the corresponding legal obligations.

9.4 Data retention period

The data processed in the European Internal Information Channel may only be retained therein for the time necessary to decide on the appropriateness of initiating an internal investigation.

In any case, three months after receipt of the report, the data will be deleted, unless the purpose of the retention is to keep a record of the functioning of the Channel or it may constitute a crime, in which case the information will be retained for as long as necessary during the legal proceedings.

9.5. Exercise of rights

Persons whose personal data are processed within the framework and context of the European Internal Information Channel will be informed about the processing of their personal data, in accordance with the terms set out in Articles 13 and 14 of the GDPR.

They may exercise their rights of access, rectification, erasure, objection, restriction and portability recognised in Articles 15 to 22 of the GDPR by writing to the following email address:dataprotection@teka.com or to the Spanish Data Protection Agency (www.aepd.es). However, when the data subject exercises the right to object, it will be presumed that, unless proven otherwise, there are compelling legitimate grounds that justify the processing of their personal data, and therefore this right will not be effective.

The right of access to personal data shall in no case cover the identity of the Whistleblower, limiting the possibility of communicating said identity solely to the judicial authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or sanctioning investigation.

9.6. Principle of proportionality and data minimisation

Only personal data that is relevant will be collected. If its relevance to the processing of specific information is not apparent or if it is collected by accident, it will be deleted without undue delay. Likewise, all personal data that has been communicated and that refers to behaviour that is not included in the scope of this Policy shall be deleted. If the information received contains personal data included in the special categories of data, it shall be deleted immediately, without being recorded or processed.

9.7 Security measures:

The European Internal Reporting Channel is designed, established and managed in a secure manner, ensuring the confidentiality of the identity of the Reporter and any third party mentioned in the report, as well as the actions taken in the management and processing of the report, preventing access by unauthorised personnel.

Thus, the European Internal Information Channel has technical and organisational measures in place to preserve the security of the data collected and the confidentiality of communications, in order to protect them against disclosure and unauthorised access.

10. Use of the European Internal Information Channel and the Policy

The European Internal Information Channel and the Policy that implements it shall be used in good faith, and the submission of false, unfounded or distorted information, as well as information that has been obtained illegally in order to harm or damage individuals or any company in its Group, shall not be considered to be in accordance with the principle of good faith or the purpose of the Policy and the applicable regulations that develop the protection of persons who report regulatory and anti-corruption infringements.

11. Non-compliance

All persons covered by this Policy are obliged to comply with its content. If a serious breach of this Policy or any other element of the European Internal Reporting Channel is identified, this can and must be brought to the attention of the System Manager.

12. Amendments

This Policy will be reviewed and updated annually, unless it is necessary to do so at an earlier date, without prejudice to the System Manager being able to make any necessary corrections, rectifications or clarifications.

This Policy replaces any previous Whistleblowing Policy approved by the Board of Directors of Teka Industrial, S.A.

13. Legal nature

This Policy complies with Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union and Council law, and with the requirements of Law 2/2023 on the protection of persons who report regulatory and anti-corruption breaches.

All of the above is without prejudice to the rest of the European regulations transposing this Directive, which shall be observed and shall apply for management and protection purposes if not expressly provided for in this Policy.

Annex I - Local reporting channel

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

Annex II: Entities covered by this Policy

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. z o.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
Midea Europe GmbH
Midea Electric France Limited Liability Company
Midea Italia Srl
Midea Home Appliances UK Ltd