TRIMAS GLOBAL INTERNAL DATA PRIVACY POLICY

Effective Date: Updated July 1, 2023

SCOPE: This Policy applies to employees of TriMas Corporation and its subsidiary companies (collectively, "TriMas") and certain agents acting on behalf of TriMas, as specified in this Policy. If you Process Personal Data (as defined below) of a TriMas entity in Europe or the United Kingdom or you are providing goods or services to, or monitoring individuals in, the European Union or United Kingdom, you are also required to comply with the requirements in Appendix A to this Policy. All capitalized terms in this Policy have the meaning in the definition section below.

PURPOSE: The purpose of this Policy is to assist TriMas personnel in complying with applicable data protection laws. This Policy establishes the process for TriMas to obtain, use, transfer and process Personal Data about individuals and to inform employees about the rules for protecting Personal Data. The Policy also describes individuals' rights in relation to Personal Data processed by TriMas or its agents processing Personal Data on TriMas' behalf.

POLICY: TriMas strives to collect, store, use, disclose and Process Personal Data in compliance with applicable laws where TriMas does business as well as in accordance with the TriMas Code of Conduct. If you are aware of or reasonably suspect any Processing of Personal Data that may violate this Policy, you are required to report such Processing by notifying your manager, Human Resources or reporting your concern to the Ethics Helpline https://secure.ethicspoint.com/domain/media/en/gui/55943/index.html.

TriMas contractors, employees, and agents (including external organizations, consultants, contractors, and service providers Processing Personal Data) that Process Personal Data are required to comply with this Policy. Employees who fail to comply with this Policy or who cause TriMas to breach data protection laws may face disciplinary action up to and including termination of employment.

Where applicable laws impose less stringent obligations for Processing Personal Data than this Policy, this Policy controls. If applicable laws impose more detailed or stricter requirements than this Policy, compliance with such laws or regulations will be expected. Specific requirements related to Personal Data from individuals located within the European Union are identified in Appendix A to this Policy.

1. Definitions

Personal Data is any information (for example, a person's name) or combination of information about a person which allows that person to be identified or identifiable from the information (for example last name and address, but also comments about them, their health status, IP address, device identifiers or employment history. This term includes the definitions of personal information, personal data, and related terms as may be relevant under applicable laws.

Processing is collecting, storing, using, disclosing, changing or processing in any other manner of Personal Data.

Sensitive Personal Data (now known in the GDPR as Special Categories of Personal Data) is Personal Data that requires enhanced protection because disclosure presents a greater risk of harm. It includes racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. While personal financial information and government issued identification numbers are outside the scope of sensitive personal data, such information should be treated with care.

Business Purposes include, but are not limited to:

- Performance under a contract with an individual

- Recruitment
- Employee administration
- Employee performance management and professional development
- Payroll and accounting functions
- Business and market development
- Financial reporting
- Customer and supplier relation management
- Technology infrastructure and support
- Facilities management
- Compliance with law, regulations and TriMas' policies
- Audits and investigations, handling legal claims and defending TriMas' interests

2. What can we do with Personal Data?

Personal Data may only be Processed for legitimate Business Purposes. In addition, its use must be both fair and lawful, which means that the individual understood why his or her Personal Data was requested and how TriMas would use that Personal Data. Fair and lawful use includes at least one of the following:

a. The individual consents to the Processing (which consent should be cautiously relied upon as addressed below).

b. It is necessary for the performance of a contract between TriMas and the individual.

c. It is necessary to comply with a legal obligation of TriMas.

d. It is necessary to protect a vital interest or life of the individual.

e. It is necessary to prevent threats to state or public security or to prosecute crimes.

f. It is necessary for a legitimate Business Purpose and the use is fair to the individual.

For example, TriMas requires personal banking information if an employee agrees to have wages deposited directly. If an employee would like to enroll in healthcare plans, TriMas, or its agents, would require disclosure of Personal Data.

Processing Sensitive Personal Data may require additional protections required by law, and another legal justification in addition to one of "fair and lawful use" justifications listed immediately above. For example, some laws require explicit consent of the individual. When Processing Sensitive Personal Data, contact the TriMas Legal Department to ensure compliance with applicable laws, and review Appendix A to this Policy regarding the Processing of Personal Data with respect to European Union based personnel.

3. How much Personal Data is collected and how long is it maintained?

The following basic principles govern the scope of Personal Data that can be collected and how long it can be kept.

a. TriMas shall only collect the amount of Personal Data necessary to achieve the related documented Business Purpose.

b. TriMas shall take reasonable steps to ensure Personal Data is accurate, current and reliable for its intended use.

c. TriMas employees must take care to record, input and update Personal Data accurately. Some Personal Data may change from time to time (such as addresses, contact details and bank accounts).

d. Some records, including Personal Data, must be retained for minimum periods by law (such as payroll records). Record retention periods are set forth in the TriMas Records Retention Policy for records maintained in the U.S. and certain other jurisdictions. In all cases, TriMas will comply with local laws and otherwise maintain the records for only so long as those records are used for a legitimate Business Purpose.

4. How does TriMas protect Personal Data?

The following principles apply with respect to the protection of Personal Data:

a. TriMas shall secure all Personal Data that it Processes through appropriate administrative, technical and physical security measures to appropriately protect such Personal Data from loss, theft, misuse and unauthorized access, modification, disclosure or destruction. For more information about the security measures necessary to protect Personal Data and avoiding breaches, see TriMas' Global Electronic Communications Policy and local security procedures and policies.

b. Any individual responsible for a system containing Personal Data that may have been compromised shall take immediate steps to secure that system and notify a supervisor and IT personnel immediately.

c. All personnel are responsible for the protection of Personal Data and only those authorized consistent with their role and responsibilities may Process Personal Data.

d. Extra care should be exercised with respect to Sensitive Personal Data.

5. Security measures deployed to protect Personal Data (or Sensitive Personal Data)

Protecting Personal Data (or Sensitive Personal Data) requires effort on the part of every TriMas employee and the deployment of best practices, including the following:

a. Do not send such data to a party outside of TriMas unless it is encrypted or password protected (consider using a secure data sharing portal instead).

b. Protect access to such data, electronic and paper, by limiting the ability of unauthorized individuals to view it. Do not leave it on your desk, in plain view on your computer screen or view it in a public place. Avoid downloading Personal Data to a mobile device.

c. Password maintenance and security for all devices must comply with TriMas policy.

6. Can Personal Data be provided to third parties?

Personal Data may be disclosed to third parties:

a. For a Business Purpose and with an appropriate contract with the third party ensuring the security of Personal Data;

b. As required by applicable laws or regulations;

c. Where necessary to perform contractual obligations with the individual concerned subject to reasonable security measures; and/or

d. With the consent of the individual concerned.

Third parties who receive Personal Data are required to guarantee protection of Personal Data and to comply with data protection laws in all countries where Processing is performed. Please consult with the Legal Department prior to entering into a contract involving the disclosure of personal data to a third party.

TriMas uses third parties to provide services, for example, running IT systems, payroll processing, legal advice, benefits administration and other support. When a third party will use TriMas employees' Personal Data, it must have a written contract with TriMas with specific limitations on its use of the Personal Data and requiring appropriate security. Contact the TriMas Legal Department regarding appropriate contractual language.

7. Can Personal Data be transferred internationally?

TriMas may transfer Personal Data to a TriMas affiliate located in another country for legitimate Business Purpose, when it complies with fair and lawful use of the Personal Data and when the receiving entity ensures that the Personal Data will be appropriately Processed and protected.

Further to its commitment to comply with relevant data protection laws, TriMas shall make required notifications to data protection authorities or obtain authorizations related to Processing of Personal Data. Some countries have special rules transferring Personal Data to another country. For example, within the European Economic Area, there are restrictions on the transfer of Personal Data to make sure the Personal Data remains safe, and individuals do not lose protections under local law. When sending Personal Data outside of the European Economic Area, review Appendix A and contact the TriMas Legal Department to ensure that transfers comply with local law.

8. What are individuals' rights to their Personal Data?

Individuals have different rights depending on their residency. TriMas personnel must forward any data subject rights requests received to the TriMas Legal Department as quickly as possible upon receipt. In general, TriMas strives to provide all individuals with the following rights regarding their Personal Data:

a. The right to access their Personal Data (for example, through access to a third party provider's system or viewing their personnel file).

b. The right to prevent Processing of Personal Data for direct marketing purposes.

c. The right to have Personal Data corrected and/or deleted where appropriate (for example, updating home address).

d. The right to not be discriminated against for exercising their Personal Data rights.

If an individual requests information about his or her Personal Data, TriMas will comply with the regulatory requirements related to this request. TriMas entities operating in the European Union are bound by additional rights as set out in Appendix A, which also apply to European Union citizens regardless of where their personal data is Processed**.**

In the event that any TriMas contractor, employee, or agent receives a purported or suspected individual rights request, that person must notify their manager, Human Resources, or the Legal Department regarding the request.

9. What should I do if I lose Personal Data or I think there is a data security breach?

There are potentially significant repercussions for TriMas and the individuals affected arising from a security breach. If you believe Personal Data may have been lost or stolen:

a. Immediately report the details to your Human Resources representative or the TriMas Legal Department;

b. Follow guidance relating to the security breach in TriMas Incident Response Plan; and

c. **Do not disclose any information regarding any actual or suspected breach to any parties outside of the TriMas Legal Department**. Do not approach any individual data subjects, customers or regulators or make any public announcements about any potential or actual security breach incident.

In the event of an actual or suspected breach, time is of the essence. Please notify the Legal Department immediately so that TriMas may begin mitigating risks associated with a breach as quickly as possible.

10. What about the use of Personal Data for marketing purposes?

As with other types of Processing, the use of Personal Data for marketing purposes must satisfy the fair and lawful use requirements set out above. Typically, this will mean consent by the recipient. You should not use Personal Data to contact individuals for marketing purposes by email, text or any other method unless the individual has consented or been made aware that it will happen. Individuals have a right to decline direct marketing at any time.

Please note that California provides its citizens with the right to request that we not sell or share their personal information through the California Consumer Privacy Act ("CCPA"). Any requests, questions, or complaints received regarding the CCPA should be sent to the Legal Department immediately.

Where marketing is by email, text or similar means, the consent/awareness must clearly cover marketing by these means. Special rules may apply to how consent is obtained (for example, whether individuals can "opt out" of or "opt in" to receiving marketing) depending on the type of marketing and the means of communication with the individual. If you have specific questions about using Personal Data for marketing, contact the TriMas Legal Department. For marketing undertaken regarding European Union citizens, see Appendix A.

Appendix A

European Union and United Kingdom Data Privacy Requirements

In 2018, the European Union passed the General Data Protection Regulation, which provides data subjects with rights regarding their Personal Information and governs how TriMas is permitted to Process Personal Information. Following Brexit, the United Kingdom passed its own version of the General Data Protection Regulation, which is substantially similar to its EU counterpart. This policies refers to these laws collectively as the "GDPR."

All Company Personnel must comply with the GDPR and familiarize themselves with our relevant internal policies and procedures for securely handling Personal Data. Failure to comply with the GDPR could result in fines to TriMas of up to 4% of annual global TriMas group sales, claims by those affected by a breach, and significant reputational damage. Any breach of this policy or Related Policies may result in disciplinary action up to and including termination. There may also be personal criminal sanctions for some compliance failures, such as unauthorized obtaining of data or failing to assist a regulator.

TriMas may supplement or amend this Policy from time to time. The TriMas Legal Department is responsible for overseeing this Policy. Contact your supervisor or the TriMas Legal Department with any questions about this Policy or the GDPR.

This policy applies to all Personal Data created or processed by or for TriMas entities to deliver services and conduct business, recruitment, employment and operations, including information received from or exchanged with external partners. The Policy applies to information regardless of its medium (electronic or hard copy) and may also determine what can be communicated verbally to third parties.

Personal Data can take many forms including, but not limited to, the following:

- Hard copy data held on paper (when in a structured filing system)
- Data stored electronically in computer systems and mobile devices (e.g., smart phones)
- CCTV footage, as regulated by our CCTV Policy
- Communications sent by physical post or using email
- Data stored using electronic media such as USB drives, servers, disks and tapes
- Data stored in the cloud (e.g., file sharing sites) and social media

Always contact the TriMas Legal Department in the following circumstances (see the Section on Data Processing for further details):

- if you are **unsure of the lawful basis** which you are relying on to process Personal Data (including the legitimate interests used by the Company) (see Data Processing in this Appendix);
- if you **need to rely on Consent** and/or need to **capture Explicit Consent** (see Consent in this Appendix);
- if you need to **draft Privacy Notices** or **Fair Processing Notices**;
- if you are **unsure about the retention period** for the Personal Data being Processed (see Data Retention in this Appendix);
- if you are **unsure about what security** or other measures you need to implement to protect Personal Data;
- if there has been a **Personal Data Breach** (see Breach Reporting in this Appendix);

- if you **intend to transfer data subject to the GDPR** to a country that has not been deemed as providing adequate security measures for Personal Data (e.g., the United States);
- if you are unsure on **what basis to transfer** Personal Data outside the European Economic Area;
- if you need any assistance **dealing with any rights** invoked by a Data Subject (see Rights of Data Subjects in this Appendix);
- whenever you are engaging in a significant new, or change in, **Processing activity** which is likely to require a Data Protection Impact Assessments (DPIA) or plan to use Personal Data for **other purposes** than what it was collected for;
- if you plan to undertake any activities involving **Automated Processing** including profiling or **Automated Decision-Making;**
- if you need help complying with applicable law when carrying out **direct marketing activities** (see the Section on Direct Marketing in this Appendix); and/or
- if you need help with any contracts or other areas in relation to **sharing Personal Data** with third parties (see Outsourcing / Suppliers in this Appendix).

1. Definitions

Capitalized terms used in this Policy are defined in Annex A.

2. Governance

Policy Dissemination & Enforcement

The management team of each TriMas entity must ensure that all Employees responsible for the Processing of Personal Data are aware of and comply with the contents of this policy. In addition, TriMas entities will make sure all Third Parties engaged to Process Personal Data on TriMas' behalf (i.e. their Data Processors) are aware of and comply with the contents of this Policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to Personal Data controlled by TriMas entities or otherwise permitting them to process any Personal Data on TriMas' behalf.

Audit – Compliance Monitoring

To confirm compliance with this Policy, TriMas is committed to undertaking Data Protection compliance audits as more fully set forth in Annex B.

3. Data Protection by Design

Introduction

Data protection by design provides a method for proactively embedding privacy into information technology, business practices, and networked infrastructures to ensure that data is managed through a lifecycle to ultimate data deletion.

TriMas entities have a general obligation to implement technical and organizational measures to show consideration and integration of data protection into processing activities. The focus is proactive instead of reactive data protection design. Privacy and data protection should be considered in the early stages of any project and then throughout the project lifecycle.

The GDPR approach

The GDPR recommends taking a risk-based approach to data protection by design.

Taking into account the state of the art, the cost of implementation and the nature, risk, scope, context and purpose of processing, TriMas entities must implement appropriate technical and organizational measures, such as pseudonymisation, to integrate the necessary safeguards to meet the GDPR requirements.

Checklist for implementing Data Protection by Design

1. Review and apply data protection by design and the Data Protection principles - review the users of personal data within the business and ensure that their processing applies data protection by design and core data protection principles. The relevant TriMas entity's Data Inventory will be a useful starting point.
2. Review privacy and security throughout the data lifecycle (e.g., collection, use, retention, storage, disposal or destruction).
3. Determine which data uses require identifiable data - use anonymised or pseudonymised data where possible.
4. The data protection by design team, is responsible for process focus and awareness with respect to data protection by design.
5. Create or update gateways in decision-making processes to include data protection considerations.
6. Update process manuals to include early data protection involvement.
7. Apply DPIAs for high risk processing (see below for more details).
8. Consider external accreditation so processes and procedures adhere to known standards.

Benefits

The benefits of data protection by design include the following:

- Minimizing compliance risk as issues are identified at an earlier and less costly stage;
- Fostering industry and workplace confidence; and
- Reducing the chance of high-profile data breaches.

In completing a DPIA, a TriMas entity will work with the TriMas Legal Department, the IT department and, as necessary, external advisors, Data Protection Principles.

The following data protection principles are key to compliance with the GDPR.

Principle	Definition
Fairness and transparency	TriMas entities must advise the Customer or Employee of the intended use of the Personal Data (transparency) and Process that data in accordance with the intended use (fairness) contained within a fair processing notice or Company Privacy Policy, and one of the lawful grounds set out in the GDPR must apply (lawfulness).
Purpose limitation	TriMas entities must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data consistent with the specified purpose.
Data minimization	TriMas entities must not collect or store any Personal Data beyond the applicable requirements, and take pro-active steps to achieve this, including converting personal data into anonymized data or pseudonymised data where possible. Privacy settings and controls should be set to a default of not collecting non-essential Personal Data.
Accuracy	TriMas entities must have in place processes for identifying and addressing out-of-date, incorrect, incomplete and redundant Personal Data.
Storage limitation	TriMas entities must, wherever possible, store Personal Data in a way that limits or prevents identification of a Customer or Employee. Personal

	Data should not be retained for longer than necessary in relation to the purposes for which it was collected.
Security, Integrity and Confidentiality	TriMas entities must use appropriate technical and organizational measures to maintain the integrity and confidentiality of Personal Data.
Transfer limitation	TriMas entities must not transfer Personal Data to another country without appropriate safeguards.
Data Subjects' Rights and Requests	TriMas entities must make Personal Data available to Data Subjects and Data Subjects have certain rights in relation to their Personal Data.
Accountability	TriMas entities must be able to demonstrate compliance with the data protection principles listed above.

4. Accountability

TriMas entities must demonstrate the data protection principles (outlined in Section 4 above) are satisfied for all covered Personal Data.

TriMas entities have put in place a number of processes to achieve accountability, including:

- Operation of a data privacy governance structure led by the TriMas Legal Department to oversee compliance, supported by a governance structure;
- Maintaining an accurate and up to date data inventory of data processing activities ;
- Implementing appropriate privacy notices;
- Obtaining appropriate consents;
- Applying appropriate organizational and technical measures for compliance with the Data Protection principles, such as policies and training;
- Carrying out Data Protection Impact Assessments; and
- Creating a breach reporting mechanism.

5. Data Processing

PERSONAL DATA

TriMas entities use the Personal Data of its Customers and employees and contacts for its Business Purposes.

The use of an individual's information should always be considered from his or her perspective, including whether the use will be within the individual's expectations or if the individual is likely to or could reasonably be expected to object.

TriMas entities will Process Personal Data in accordance with all applicable laws and contractual obligations. In particular, TriMas entities will not Process Personal Data unless at least one of the following requirements is met and reflected in the Privacy Notice and data inventory:

a. The Customer has given **Consent** to the Processing of its Personal Data for one or more specific purposes.

b. Processing is necessary for the **performance of a contract** to which the Customer is party or in order to take steps at the request of the Customer pr**ior to entering into a contract (such as a contract of sale / employment contract).**

c. Processing is necessary for compliance with a **legal obligation** to which TriMas entities are subject **(such as to prevent or detect a crime or fraud, reporting earnings to tax authorities)**.

d. Processing is necessary in order to protect the **vital interests (i.e. life or death)** of an individual **(such as disclosing pertinent information to emergency services in relation to a unconscious member of staff)**

e. Processing is necessary for the purposes of the **legitimate interests** pursued by the **Customer or by a Third Party** (**except where such interests are overridden** by the interests or fundamental rights and freedoms of the Customer).

There are some legitimate circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected, but where this is likely or being considered, consult the TriMas Legal Department.

SPECIAL CATEGORIES OF PERSONAL DATA

In some cases where we Process Special Categories of Personal Data, the Data Subject's explicit consent is required, unless one of the other justifications below applies. Where consent is relied upon, the consent must identify the relevant data, why it is being processed and to whom it will be disclosed. TriMas entities will only Process Special Categories of Personal Data in accordance with applicable law and record it in the applicable Privacy Notice and the data inventory, where at least one of the following non-exhaustive criteria applies:

a. The Customer or Employee has explicitly consented.

b. The Personal Data has been made public by the Customer or Employee.

c. Processing is necessary for occupational health or other care.

d. Processing is necessary for legal claims or where courts are acting in their judicial capacity.

e. Processing is authorized or required by law (for example employment law / social protection law).

f. Processing is necessary for historical research or statistical purposes and safeguards have been put in place to protect Customers/Employees.

g. Processing is necessary to protect the vital interests (this essentially applies in a "life or death" scenario) where the Data Subject is physically or legally incapable of giving Consent.

Where Special Categories of Personal Data are being Processed, TriMas entities must adopt additional measures to protect the data (such as encryption).

If you have any concerns regarding the processing of Special Categories of Personal Data, contact the TriMas Legal Department.

CONSENT

The GDPR sets a **higher standard for consent to Process Personal Data.** Consent means offering choice and control over how one's Personal Data is used. The Personal Data collected after receiving consent remains subject to a Data Subject's ability to revoke consent at any time. Consult with the TriMas Legal Department as necessary regarding the use of consent. Consent is generally not an appropriate basis for Processing Personal Data in the Employment Context. TriMas should avoid Processing Personal Data exclusively on the basis of Consent unless necessary.
Consent must be:

- **Unbundled**: Consent requests must be separate from other terms and conditions and should not be a precondition of signing up to a service unless necessary for that service.
- **An active opt-in**: Consent must be expressed by a statement or clear affirmative action. Silence, pre-ticked boxes or inactivity should not constitute consent, and pre-ticked opt-in boxes are invalid – use unticked opt-in boxes or similar active opt-in methods.
- **Granular**: granular options must be provided allowing Data Subjects to consent separately to different types of consent-based Processing wherever appropriate.
- **Named**: the relevant TriMas entities and/or any third parties who will be recipients of the Customer or Employee's Personal Data must be named.
- **Documented:** Records must be maintained to demonstrate the Data Subject's consent, including what they were told, and when and how they consented (e.g., timestamp and the form of words) and if they withdrew consent.
- **Easy to withdraw**: Data Subjects have the right to withdraw consent and it must be as easy to do so as it is to give consent. Simple and effective withdrawal mechanisms must be in place (e.g., unsubscribe link or contact number).
- **No imbalance in the relationship**: Consent will not be freely given if there is imbalance in the relationship between the Data Subject and TriMas entities. Consent from an Employee will except in rare cases be invalid due to imbalance considerations.
- **Plain Language:** The consent language must be intelligible, clear and simple.

6. Direct Marketing

We are subject to certain rules and privacy laws when marketing to our customers and contacts. We can send direct marketing to corporate entities without consent, but we need to ensure that we respect individuals' rights and we are clear as to how Personal Data is being used. The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner and clearly distinguishable from other information. A Data Subject's objection to direct marketing must be honored. If a Data Subject opts out, suppression of the Data Subject's Personal Data should be promptly implemented (meaning no further communications are sent).

7. Rights of Data Subjects and our obligations to them

Under the GDPR, individuals have certain rights, including the right to request access to any data held about them. These rights, summarized in the table below, can be exercised at any time by a Data Subject, including Customers or Employees. Data Subjects are not required to provide an explanation for

exercising this right under the GDPR. Any such requests should be directed to the TriMas Legal Department. TriMas personnel and agents are prohibited from attempting to comply with or fulfill such requests on their own without express authorization from TriMas Legal.

Right	Description
To be informed about processing (transparency)	In the EU, individuals have right to notices about TriMas' Processing of their Personal Data ("Privacy Notices", also known as "Fair Processing Notices"). Fair Processing Notices contain detailed information about the purposes and manner of processing Personal Data, the legal basis on which the processing takes place, how data is used and shared, whether it is transferred around the world, the Data Subject's rights noted below and how to make complaints.
Information Access	Data Subjects have a right to request a copy of their Personal Data being Processed by a TriMas entity together with supplementary information which includes information on the likely external recipients of the data, how long the information will be retained, the source of the data (if from other than the Data Subject), the existence of other rights detailed in this section and the right to complain to appropriate regulatory bodies.
Objection to Processing	Data Subjects have the right to object, on grounds relating to their particular situation, to the processing of their Personal Data unless TriMas can demonstrate that it either has compelling grounds for continuing the Processing, or that the processing is necessary in connection with its legal rights.
Objection to automated decision making (including Profiling)	Data Subjects have the right not to be subject to a decision based solely on automated processing (e.g., in connection with offers of employment; discounts; insurance premiums) which significantly affect them (including profiling). Such processing is permitted where it is necessary for entering into or performing a contract with the Data Subject provided that appropriate safeguards are in place, it is authorized by law or the Data Subject has explicitly consented and appropriate safeguards are in place. A common example of automated decision making would be the automatic refusal of an employment application using a risk-score based model.
Right to Withdraw Consent	Data Subjects have the right to withdraw consent to Processing of Personal Data based on Consent, as noted above.
Restriction of Processing	Data Subjects have the right to restrict the Processing of Personal Data (meaning that the data may only be held by TriMas entities, and may only be used for limited purposes) if the accuracy of the data is contested (and only for as long as it takes to verify that accuracy), the Processing is unlawful and the Data Subject requests restriction (as opposed to exercising the right to erasure), the data is no longer needed for its original purpose, but the data is still required by TriMas entities to establish, exercise or defend legal rights.
Data portability	A Data Subject has the right to receive a copy of his or her Personal Data in a common, structured electronic and reusable format. A Data Subject may

	also request that his or her Personal Data be transferred directly to another organization.
Data Rectification	TriMas entities must ensure that inaccurate or incomplete Personal Data is erased or rectified.
Right to be forgotten	A Data Subject may request that his or her Personal Data be deleted or removed, which right is limited and subject to review by TriMas or the Third Party, as the case may be, as to whether an exemption applies. This is however a limited right and specific guidance should be sought. Any Third Parties who Process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Written requests from any party submitting a request about his or her Personal Data should be forwarded to the TriMas Legal Department to determine whether a compliance exemption applies and maintain an appropriate record of all such requests.

Fee

In certain limited circumstances, a fee can be charged for compliance with a data request, determination of which should be made in consultation with the TriMas Legal Department.

ID & Verification

Data Subjects must provide proof of identity before exercising data request rights to limit the risk that Third Parties gain unlawful access to Personal Data.

Time limit

Response to data requests must be addressed within 30 days of receipt of the written request, which period may be extended by 60 days due to complexity and volume.

Law Enforcement Requests & Disclosures

TriMas entities are permitted to share information about Data Subjects, including Customers or Employees, with law enforcement and government agencies without the knowledge or consent of a Data Subject, for any of the following purposes:

- The prevention or detection of crime;
- The apprehension or prosecution of offenders;
- The assessment or collection of a tax or duty; or
- By the order of a court or by any rule of law.

8. Data Quality

Personal Data collected must be complete and accurate and updated to reflect the current situation of the Data Subject. Personal Data should be validated and updated on a regular basis.

Personal Data known to be incorrect, incomplete, ambiguous, misleading or outdated, even if provided by the Data Subject, must be corrected.

9. Data Retention

Personal Data relating to all Data Subjects must be deleted or destroyed if there is no longer a reason to retain it.

The length of time for which TriMas entities must retain Personal Data is set out in our Retention Policy.

10. Storing Data Securely

Personal Data must be protected against undesired destruction or loss and all TriMas personnel are responsible for understanding TriMas' information security policies.

11. Breach Reporting

All TriMas personnel (including temporary workers) must promptly report actual or potential Data Protection breaches or compliance failures to a supervisor or directly to the TriMas Legal Department.

A Personal Data breach *could* be caused by a number of events, including:

- theft of a laptop;
- loss of a USB containing Customer records;
- emailing records containing Personal Data to improper recipients;
- printing Personal Data of customers or Employees and failing to control the printed materials;
- phishing or vishing attack which allows a third party to access company systems or records;
- malicious hacking;
- an Employee or consultant accessing Employee Personal Data records without authorization to do so.

TriMas' data breach notification policy is set out in TriMas' Incident Response Plan.

12. Outsourcing/Suppliers, Data Sharing and Data Transfers

Suppliers

TriMas'suppliers with access to Personal Data must certify in writing compliance with the GDPR and implementation of appropriate technical and organizational security measures. TriMas may only transfer Personal Data to, or allow access by, Third Parties when such Third Party undertakes that any such Personal Data will be processed legitimately and protected appropriately.

Contracts

All relationships with Third Parties regarding the transfer or processing of Personal Data must be covered by an appropriate agreement requiring the Third Party to protect the Personal Data, promptly report data breaches and to only Process Personal Data in compliance with TriMas instructions. Please consult with the TriMas Legal Department to ensure appropriate contracts are put in place prior to transferring Personal Data to a vendor or other third party.

Transfers of Data outside the European Economic Area (EEA)

Personal Data may not be transferred to any individual or company located outside the European Economic Area or United Kingdom without the prior written approval of the TriMas Legal Department. This limitation applies where a company uses equipment, resources or a subcontractor located outside the European Economic Area to process Personal Data. Some transfers of Personal Data within TriMas are covered by the specific provisions of an intra-group agreement which applies to transfers of Personal Data to TriMas in the United States, Brazil, China, Mexico, Singapore and certain other countries in which TriMas does business because these countries are not viewed as having adequate protection by European Economic Area standards for Processing of Personal Data.

For the avoidance of doubt, TriMas must ensure that Restricted Transfers of Personal Data, as defined by Chapter 5 of the GDPR, are subject to appropriate transfer mechanisms, as required by the GDPR. It is the duty of the TriMas Legal Department to identify and implement appropriate transfer mechanisms, such as standard contractual clauses.

Audits

Regular audits of the information security measures of Third Parties handling TriMas data (including any Personal Data), especially with respect to information security measures must be undertaken. Any major deficiencies identified will be reported to and monitored by the TriMas Legal Department. Audit scope is addressed in Annex B.

13. Data Protection Training

All current and future personnel (including temporary workers) must receive training on this Policy which training will updated as necessary.

14. Complaints Handling

All complaints received in writing regarding the Processing of Personal Data will be investigated by the TriMas Legal Department and the complainant will be informed of the progress and outcome of the complaint within a reasonable period.

TriMas will seek to resolve any complaints relating to the Processing of Personal Data promptly and fairly and will cooperate with data protection authorities in resolving any such complaints.

Absent resolution with a complainant, the complainant will be advised that it may, at its discretion, seek relief from the applicable data regulator.

15. Deviations

Any deviation from this policy requires prior written approval from the TriMas Legal Department.

Annex A – Glossary of Terms

TERM	DEFINITION
Anonymisation	Personal Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person, and such that the data cannot be linked to an individual.
Company Personnel	Includes all employees, third party contractors and representatives.
Customer	Any past, current or prospective customer of a company within TriMas.
Consent	Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.
Data Controller	An organization (or person in exceptional circumstances) which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Data Subject	Anyone 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Protection	The process of safeguarding Personal Data from unauthorised or unlawful use, disclosure, access, alteration, processing, transfer or destruction.
Data Protection Impact Assessment or DPIA	A Data Protection Impact Assessment is an assessment to identify and minimise any risks associated with the Processing of Personal Data.
Data Processors	An organization (or person in exceptional circumstances) which Processes Personal Data on behalf of a Data Controller.
Employee	An individual who works part-time or full-time for a company within TriMas under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties, including temporary employees and independent contractors.
Encryption	The process of encoding a message or information in such a way that only authorized parties can access it.
Information Commissioner's Office (ICO)	An independent public authority in the UK responsible for monitoring the application of the relevant UK Data Protection laws and regulations.

Personal Data	Personal Data is any information about any living, identified or identifiable individual. The company is legally responsible for this and its storage, protection and use are governed by the General Data Protection Regulation and associated laws.
Process, Processed, Processing	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include collection, storage, access/use, disclosure, erasure.
Related Policies	Includes: the policies found at https://triconnect.trimascorp.net/Legal/Pages/Home.aspx, plus as applicable policies which refer to or relate to the processing of Personal Data.
Sensitive Personal Data	Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data or criminal offences or convictions.
Third Party	An external organisation with which TriMas conducts business and is also authorised to, under the direct authority of TriMas, to process the Personal Data of Customers, Employees or other Data Subjects on its behalf.
Third Country	Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.

Annex B – Data Protection Compliance Audit – to be addressed in Quarterly meeting

Data Protection Compliance Audits help to assess whether TriMas is following good Data Protection practice and meeting its Data Protection obligations.

Each audit will, at a minimum, assess compliance with this and Related Policies and the operational practices in relation to the protection of Personal Data, including:

- The assignment of responsibilities;
- Raising awareness;
- Training of Employees;
- Adequacy of organizational and technical controls to protect Personal Data;
- Records management procedures (including data minimization);
- Adherence to the qualified rights of the Data Subject;
- Privacy by design and default;
- Consent/permissions for direct marketing;
- Personal Data transfers;
- Personal Data incident management (including Personal Data breaches);
- Personal Data complaints handling;
- The currency of Data Protection policies and privacy notices;
- The accuracy of Personal Data being stored;
- The conformity of Data Processor activities;
- The adequacy of procedures for redressing poor compliance; and
- The security of Personal Data in transit and when at rest.

Any major deficiencies identified will be reported to and monitored by the TriMas Legal Department.