Global Data Privacy Compliance Statement

Matthews International Corporation, including all subsidiaries and affiliates (collectively, "***MATW***"), have a deep awareness and understanding of the importance that our customers and business partners place on data privacy and security. MATW considers this a priority as well.

In recent years, many countries have enacted data privacy and security regulations and laws, such as the California Consumer Privacy Act ("***CCPA***")* or the General Data Protection Regulation of the European Union ("***GDPR***")** and other laws. With each new law and regulation relating to data privacy and security, we undertake a systematic review of our data processing practices and procedures on a global basis and across our entire group of companies. As an evolving global organisation, we continually adjust and improve our data handling practices and business offerings to meet our legal obligations as well as protect the rights and meet the needs of our employees, customers and business partners. This is an integral part of how we do business.

Key actions we undertook and are constantly undertaking in close collaboration with legal experts and will continue to undertake in the future, include:

- Reviewing our product and service offerings and how we process personal data, to determine the appropriate legal bases for processing.
- Reviewing and updating relevant privacy notices and disclaimers as needed, to ensure that we clearly explain to customers and business partners how we process their personal data.
- Putting comprehensive intragroup and international data transfer mechanisms in place and keeping them under review for exchange of data between MATW entities and external recipients.
- Reviewing the technical and organizational security measures we have implemented to protect personal data, and keeping them under review in accordance with industry best practices.
- Updating our policies, procedures and technical capabilities to respond to individuals' data subject requests.
- Reviewing our agreements with third parties that process personal data on our behalf, to ensure compliance with legal obligations, as well as our own standards on data privacy and security, so as to protect personal data adequately.
- Considering the exchange of personal data with third parties, and whether any data flows constitute "sales" of personal data under laws such as the CCPA, triggering additional obligations thereunder.
- Identifying privacy compliance-related responsibilities within the business and appointing privacy professionals, such as data protection officers.
- Updating our internal policies, procedures and controls to ensure that they reflect necessary privacy compliance requirements.

- Driving awareness and best practices, e.g., by delivering training to MATW's staff, regarding the importance of data privacy and security.
- Obligating MATW's staff to honor confidentiality, data privacy and security compliance policies.
- Further strengthening our data protection impact assessment and privacy by design programs for product and service launches and/or innovations.

In addition, MATW continuously monitors the data privacy and security landscape, including the latest guidance issued by data privacy authorities to ensure that MATW's privacy practices and procedures are kept-up-to-date.

For further questions, please do not hesitate to contact us at **privacy@matw.com**.

*** CALIFORNIA CONSUMER PRIVACY ACT (the "*CCPA*")**

The CCPA originates from the State of California within the United States but has broad applications and consequences for all of MATW's operations. Specifically, the CCPA requires companies to provide disclosures to California consumers surrounding the collection of personal information, the purpose for its collection, and selling and sharing practices. Further, the law provides certain rights to consumers, including:

- The right to know what personal information is collected;
- The right to know whether their personal information is sold or disclosed and to whom;
- The right to opt-out of the sale of their personal information;
- The right to access their personal information;
- The right to request the deletion of their personal information; and
- The right to equal service and price, regardless of whether they exercise their privacy rights.

The CCPA applies generally (barring any enumerated exemption) to for-profit businesses that collect and control California residents' personal information, do business in the State of California, and: (a) have annual gross revenues in excess of $25 million; or (b) receive or disclose the personal information of 50,000 or more California residents, households or devices on an annual basis; or (c) derive 50 percent or more of their annual revenues from selling California residents' personal information. The CCPA also demands compliance of parent companies and subsidiaries of such businesses that share their branding.

Under the CCPA, consumers protected by this Act are broadly defined as any natural person who is a California resident. A consumer's "personal information" is broadly defined to include information that identifies, relates to, describes, or could reasonably be linked, directly or indirectly to a particular consumer or household. This personal information includes, but is not limited to, the following:

- identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, e-mail address, account name, Social Security number, driver's license number, passport number, or other similar identifiers;

- characteristics of protected classifications under California or federal law;
- commercial information, including records of personal property; products or services purchased, obtained, or considered; or other purchasing or consuming histories or tendencies;
- biometric information;
- internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet web site, application, or advertisement;
- geolocation data;
- audio, electronic, visual, thermal, olfactory, or similar information;
- professional or employment-related information;
- education information;
- inferences drawn from any of the information collected to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Specifically excluded from the definition of "personal information" is any information publicly available, meaning any information that is lawfully made available from state, federal, or local government records. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

**** EU GENERAL DATA PROTECTION REGULATION (the "*GDPR*")**

The GDPR was introduced by the European Union (the "EU") and similar to the CCPA, has broad applications and consequences for all of MATW's operations, both in the EU and throughout the world. The GDPR requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. The GDPR also regulates the exportation of personal data outside the EU. Any European citizen that has their data collected by a company is a *data subject* under the GDPR, and the company that processes their data is known as the *data controller*. If a third-party is employed to handle data processing (such as a payroll company), they are the *data processor*.

The GDPR provides an array of new rights to data subjects, notably including:

- The Right to be Informed: Transparency in data collection practices means individuals have the right to be fully informed about the collection and use of their personal data.
- The Right of Access (Article 15): Individuals can request to view any personal data that has been collected from them.
- The Right to Rectify Information (Article 16): If data collected about an individual is inaccurate, the individual has the right to request a correction (rectification).
- The Right to Erasure / The Right to be Forgotten (Article 17): After information has been collected about them, individuals can request it be permanently deleted, either because the information is no longer relevant, or because the user chooses to withdraw their consent.

- The Right to Restrict Data Processing (Article 18): An individual can request to limit how their data is processed when certain conditions apply, such as if the processing is unlawful or if the individual has objected to it.
- The Right to Data Portability (Article 20): When users request to view their data, it must be given to them in a clear format so it can be easily transferred to another organization.
- The Right to Object (Article 21): Individuals can object to the processing of their data in certain situations, such as direct marketing.

The GDPR sets out guidelines regarding how data controllers (such as companies like MATW) should process personal data of data subjects (individuals), and assigns powers to regulators to ask for demonstrations of accountability, and to impose fines where requirements are not met. Requirements and guidelines include, but are not limited to, the following:

1. Lawful, fair and transparent processing
    - *Lawful* means all processing should be based on a legitimate purpose.
        - Processing personal data is lawful if at least one of the following is true:
            - The data subject has given consent
            - Processing is necessary for the performance of a contract
            - Processing is necessary for compliance with a legal obligation
            - Processing is necessary to protect vital interests of the data subject
            - Processing is necessary for the performance of a task carried out in the public interest
            - Processing is necessary for the interests pursued by the data controller
    - *Fair* means companies take responsibility and do not process data for any purpose other than the legitimate purposes.
    - *Transparent* means companies must inform data subjects about the processing activities on their personal data.
2. Limitation of purpose, data and storage: The companies are expected to limit the processing, collect only that data which is necessary, and not keep personal data once the processing purpose is completed.
3. Consent: As and when the company has the intent to process personal data beyond the legitimate purpose for which that data was collected, a clear and explicit consent must be asked from the data subject. Once collected, this consent must be documented, and the data subject can withdraw consent at any moment. (Article 4)
4. Personal data breaches: The organizations must maintain a Personal Data Breach Register and, based on severity, the regulator and data subject should be informed within 72 hours of identifying the breach. (Article 33)
5. Privacy by Design: Companies should incorporate organizational and technical mechanisms to protect personal data in the design of new systems and processes; that is, privacy and protection aspects should be ensured by default. Such default will minimize data collection. (Article 25)
6. Data Protection Impact Assessment: To estimate the impact of changes or new actions, a Data Protection Impact Assessment should be conducted when initiating a new project, change, or product.

7. Data transfers: The controller of personal data has the accountability to ensure that personal data is protected and GDPR requirements met, even if processing is being done by a third party.
8. Awareness and training: Organizations must create awareness among employees about key GDPR requirements, and conduct regular trainings to ensure that employees remain aware of their responsibilities with regard to the protection of personal data and identification of personal data breaches as soon as possible.

The GDPR applies to any company that stores or processes personal information about EU citizens within EU states, even if they do not have a business presence within the EU. Specific criteria for companies required to comply are:

1. A presence in an EU country.
2. No presence in the EU, but processes personal data of European residents.
3. More than 250 employees.
4. Fewer than 250 employees but its data-processing impacts the rights and freedoms of data subjects, is not occasional, or includes certain types of sensitive personal data.

Under the GDPR, personal information is defined in Article 4 as " any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". In other words, this definition is broad and encompasses a wide range to account for any information that can be pieced together to identify an individual, even information such as social media pseudonyms, biometric data, religious beliefs, web cookies, political opinions, and/or other identifiers.