

CUSTOMER AND VENDOR PRIVACY NOTICE

Last Updated: July 3, 2023

The Graphic Packaging International group believes it is important that the representatives and personnel of our current and prospective customers, vendors and other business partners (“**you**”, “**your**”) know how we collect, process, store, share and use their personal information when we act as controller of and the party responsible for that personal information. This Privacy Notice (“**Notice**”) describes how we use such personal information when collected in connection with our offline business activities, online customer and vendor portals, trade fairs and all other activities where this Notice is posted or linked. Wherever we refer in this Notice to ‘personal information’, we mean data relating to an identified or identifiable individual or any information that allows an individual to be identified directly or indirectly, including without limitation ‘sensitive personal information’, if any, as well as personal data and sensitive personal data or equivalent terms under applicable law.

The entity that is responsible for, and controller of, your personal information is the Graphic Packaging International Holding Company group entity with which you do business (“**GPI**”, “**we**”, “**our**” or “**us**”). A list of GPI group entities is available [here](#). This Notice does not describe the personal information practices of any third parties outside the GPI group.

In addition to reading this Notice, if you reside in California, please also read the Additional Information for California Residents section below.

1. PERSONAL INFORMATION WE COLLECT, PURPOSES OF PROCESSING AND METHODS OF COLLECTION

You may provide to us, or we may collect from third parties, the following personal information about you:

- contact information, such as name, business address, telephone number, email address;
- employment information, such as job title and name of your employer or principal;
- government identifiers, such as national identification number, driver’s license number, and Social Security Number or Taxpayer Identification Number;
- financial information (bank account details);
- data related to purchasing and selling products and/or services, and any other business interactions between us; and
- electronic identification data where required for the purpose of receiving from us or delivering to us products or services (login, passwords, IP address, cookies, access and connection times), and related data concerning IT support and technology requests.

Additionally, our vendor, HICX, may indirectly collect information about you when you use their website. For more information about HICX’s use of cookies and other tracking technologies, please read their Privacy Policy available [here](#).

Where required by applicable law, we process this personal information with your consent, which may be withdrawn at any time. We process this personal information for the following purposes, and any directly related purposes:

- conducting our business with you, including performing our contractual obligations to your employer or principal, and managing our contracts with your employer or principal;
- operating and expanding our business activities, including by developing and improving the quality and diversity of our products and services;

- responding to requests and orders, answering questions, providing requested customer support, and responding to business opportunities;
- to the extent permitted by applicable law, providing you marketing materials about products, services, news, offers, promotions and events we think may be of interest to you;
- facilitating your security and safety and those of others when you visit our facilities;
- managing our technology resources (e.g., cyber-risk management, infrastructure management and business continuity);
- detecting and preventing fraud;
- carrying out corporate governance activities, training, reporting and other internal functions;
- archiving and record-keeping;
- complying with the law, including satisfying our legal or regulatory obligations and responding to lawful requests, court orders, and legal process;
- exercising, establishing and defending our legal rights, such as by asserting our rights in court;
- protecting and defending the rights or property of others; and
- planning and carrying out reorganizations, sales, investments and similar business transactions.

As a general rule, personal information will only be collected directly from you or your device. Any personal information that you do not provide to us directly is either provided by another business professional in your field (such as a colleague) or by a supplier engaged by us and specialized in managing business relationship compliance (such as for trade sanctions background checks), or is collected from publicly available sources such as company websites or professional networking sites. Where required by law, we will obtain your consent to collect your personal information from another source unless such collection is authorized by applicable law.

It is our policy to inform business partners whether it is mandatory to provide certain types of personal information. Having a business relationship with us is voluntary, but we cannot work with you without processing some personal information (such as your contact information). If you refuse to provide us with your personal information, or if consent is required and you later withdraw your consent, we may be unable to provide you with certain goods or services.

2. LEGAL BASES FOR PROCESSING PERSONAL INFORMATION

Some data protection laws (such as the Personal Information Protection and Electronic Documents Act in Canada, and Quebec's Act respecting the protection of personal information in the private sector) require us to obtain your consent for processing your personal information for some of the purposes described above. In those cases, we will obtain your consent before processing your personal information and will not rely on other legal bases.

Other data protection laws (such as the GDPR, UK GDPR, and the Nigeria Data Protection Regulation and its Implementation Framework) require us to identify a legal justification – commonly called a “legal basis” – in order to lawfully process your personal information. The Swiss data protection law requires such a justification only if the processing of personal data is otherwise impermissible, e.g., because of non-compliance with data processing principles. Those legal bases and corresponding purposes of processing are as follows:

- ***Our legitimate (overriding) interests to efficiently conduct and manage our business partner relationships, improve our products and services and expand our business:*** performing our contractual obligations to your employer or principal and managing our contracts with your employer or principal; operating and expanding our business activities, including by developing and improving the quality and diversity of our products and services; providing you marketing materials when applicable law does not require your consent; facilitating your security and safety and those of others when you visit our facilities outside the EEA, Switzerland or UK; managing

our technology resources; detecting and preventing fraud; carrying out corporate governance activities, training, reporting and other internal functions; archiving and record-keeping; complying with the law, including satisfying our non-EEA, non-Swiss and non-UK legal or regulatory obligations and responding to lawful requests, court orders, and legal process; protecting and defending the rights or property of others; exercising, establishing and defending our legal rights, such as by asserting our rights in court; and planning and carrying out reorganizations, sales, investments and similar business transactions.

- ***Compliance with EEA, Nigerian, Swiss or UK legal obligations:*** Facilitating your security and safety and those of others when you visit our facilities in the EEA, Nigeria, Switzerland or UK; and complying with EEA, Nigerian, Swiss or UK law, including satisfying our legal or regulatory obligations and responding to lawful requests, court orders, and legal process.
- ***Contract performance or pre-contractual steps taken at your request:*** Responding to requests and orders, answering questions, providing requested customer support, and responding to business opportunities.
- ***Consent:*** Providing you marketing materials about products, services, news, offers, promotions and events we think may be of interest to you, where your consent is required by applicable law.
- ***Vital Interests:*** Protecting your vital interests or those of another individual.
- ***Public Interest:*** Performing a task carried out in the public interest or in the exercise of any official public mandate vested in us.

3. SHARING AND TRANSFERS OF PERSONAL INFORMATION

We may share your personal information with the following recipients on a need-to-know basis:

- our personnel, and personnel of GPI group entities, for the purposes described in Section 1 above. A list of GPI group entities is available [here](#);
- service providers acting on our behalf, to provide administrative, management and business support services to us and our business partners, and to assist us in providing our products and services to our customers;
- our IT systems providers, cloud services providers, database providers and consultants;
- professional advisors and external lawyers; investors and other business partners; potential or prospective buyers, sellers, lenders and their respective affiliates, agents, representatives, employees and officers.

Your personal information may be transferred to recipients situated outside of your jurisdiction of residence (for example, if you live in Québec, your personal information may be transferred outside of Québec). These recipients may be located in the United States and India which are not considered to provide adequate protection to personal information under some data protection laws (notably those of the EEA, Switzerland and the UK), as well as any other jurisdiction where we do business, or where our service providers or business partners are located. If required by applicable data protection law, we may seek your consent where we need to send your data to a country without adequate data protection law.

When we transfer your personal information, whether within the GPI group or to third parties, we will where required by law protect your personal information by requiring the recipient to act in accordance with our written instructions and/or to enter into an appropriate contract (such as [the standard contractual clauses approved by the European Commission](#), [the UK standard data protection clauses](#) and similar terms approved by the Swiss data protection authority, the UK government or relevant equivalents).

We may also share your personal information with the following recipients:

- law enforcement, courts and litigants;
- government agencies, bodies and investigators;
- tax and customs authorities; and
- regulatory authorities,
- anywhere in the world where required by applicable law.

In each case, we will obtain your consent to the sharing of your personal information where we are required to do so under applicable law.

4. YOUR RIGHTS

Subject to conditions and limitations set out in applicable law, you have certain rights in relation to your personal information which vary depending on where you are located.

If you do business with any of our EEA, Swiss or UK entities, or are a Nigerian resident or citizen, you have the following rights:

- *Right to withdraw consent* – if we rely on your consent to process your personal information, you have the right to withdraw your consent at any time. For example, if you wish to opt-out of receiving electronic marketing communications, you can change your settings in your account on our customer/vendor portal, use the 'unsubscribe' link provided in our emails, or otherwise contact us directly at gdpr-privacy@graphicpkg.com and we will stop sending you communications.
- *Right of access, rectification and erasure* – you have the right to request access to and obtain a copy of any of your personal information that we may hold, to request correction of any inaccurate data relating to you or to complete incomplete data, and to request the deletion of your personal information under certain circumstances.
- *Data portability* – if we rely on your consent to process your personal information, or the fact that the processing is necessary to perform a contract to which you are party or to take steps at your request prior to entering a contract, and the personal information is processed by automatic means, you have the right to receive all such personal information which you have provided us in a structured, commonly used and machine-readable format, and also to require us to transmit it to another controller where this is technically feasible.
- *Right to restriction of processing* – you have the right to restrict our processing of your personal information (that is, allow only its storage) where:
 - you contest the accuracy of the personal information, until we have taken sufficient steps to correct or verify its accuracy;
 - where the processing is unlawful but you do not want us to erase the personal information;
 - where we no longer need your personal information for the purposes of the processing, but you require such personal information for the establishment, exercise or defense of legal claims; or
 - where you have objected to processing justified on legitimate (overriding) interest grounds (see below), pending verification as to whether we have compelling legitimate (overriding) grounds to continue processing.

Where your personal information is subject to restriction we will only process it with your consent

or for the establishment, exercise or defense of legal claims.

- **Right to object to processing (including profiling) based on legitimate (overriding) interest grounds** – where we are relying upon legitimate (overriding) interests to process personal information, you have the right to object to that processing on grounds related to your personal situation, and we will stop that processing unless we can demonstrate compelling legitimate grounds for the processing that override your interests, rights and freedoms, or we need to process the personal information for the establishment, exercise or defense of legal claims.
- **Right to object to direct marketing (including profiling)** – you have the right to object to our use of your personal information (including profiling) for direct marketing purposes, such as when we use your personal information to invite you to our promotional events.

- *Digital legacy* – If you do business with a GPI entity in France, you have the right to define (general or specific) directives regarding the disposition of your personal information after your death. If you do business with a GPI entity in Italy, in case of death, the rights described in this section may be exercised by another person who has his or her own interest (e.g., as right holder) or acts as your agent or if family reasons that need to be protected exist. You may expressly avoid the exercise of some of the above-mentioned rights by such person by contacting us as indicated in **CONTACT US**. Furthermore, you may, at any time, withdraw or modify your wishes by contacting us as indicated in **CONTACT US**.

If you are a resident of the province of Québec, Canada, you have the following rights:

- *Right to withdraw consent* – you have the right to withdraw your consent to our use or communication of your personal information at any time. For example, if you wish to opt-out of receiving electronic marketing communications, you can change your settings in your account on our customer/vendor portal, use the 'unsubscribe' link provided in our emails or text the STOP number in our SMS, or otherwise contact us as indicated in **CONTACT US** and we will stop sending you communications.
- *Right of access, rectification and erasure* – you have the right to be informed of the source of personal information we hold on you, as well as the right to request access to and obtain a copy of any of your personal information that we may hold, to request correction of any inaccurate data relating to you and to request the deletion of your personal information under certain circumstances.
- *Data portability* – you have the right to receive all such personal information which you have provided us in a structured, commonly used and machine-readable format, and also to require us to transmit it to another party you designate where this is technically feasible.
- *Right to de-indexation*: you may, in certain situations and if the legal requirements are met, require that we cease disseminating your personal information, or that we de-index any hyperlink attached to your name that provides access to your personal information.

If you are a resident of Canada, not including Québec, you have the following rights:

- *Right to withdraw consent* – you have the right to withdraw your consent to our use or communication of your personal information at any time. For example, if you wish to opt-out of receiving electronic marketing communications, you can change your settings in your account on our customer/vendor portal, use the 'unsubscribe' link provided in our emails, or otherwise contact us as indicated in **CONTACT US** and we will stop sending you communications.
- *Right of access and rectification*– you have the right to be informed of the source of personal information we hold on you, as well as the right to request access to and obtain a copy of any of your personal information that we may hold, and to request correction of any inaccurate data relating to you under certain circumstances.

Otherwise, depending upon applicable law you may have other rights, such as to withdraw your consent, correct your personal information or obtain a copy of your personal information.

Please contact us as indicated in **CONTACT US** if you wish to exercise any of your rights, or if you have any enquiries or complaints regarding the processing of your personal information.

You may also have the right to make a complaint to the relevant regulator. For example, in the EEA and UK you may lodge a complaint with the data protection supervisory authority of your habitual residence, place of work or place of alleged infringement, if you consider that the processing of your personal information infringes applicable law.

5. DATA RETENTION

We retain your personal information for only as long as necessary, which may be for the duration of the relevant business relationship to provide you with services, and in accordance with the relevant contract. We may also retain personal information for longer than the duration of the business relationship should we need to retain it to protect ourselves against legal claims, use it for analysis or historical record-keeping, or comply with our information management policies and schedules, or as may be permitted or required by applicable laws.

6. HOW WE SECURE YOUR PERSONAL DATA

We have put in place what we consider to be appropriate security measures to prevent your personal information from unlawful or unauthorized processing and accidental loss, destruction or damage. To prevent unauthorized access to your information, we have implemented controls and security safeguards at the technical and operational levels. Our customer and vendor portals use Secure Sockets Layer/Transport Layer Security (SSL/TLS) to ensure secure transmission of your personal information. You should see the padlock symbol in your URL address bar once you are successfully logged into the portal. The URL address will also start with https:// depicting a secure webpage. SSL applies encryption between two points such as your PC and the connecting server. Any data transmitted during the session will be encrypted before transmission and decrypted at the receiving end. This is to ensure that data cannot be read during transmission. However, please note that in relation to any personal information you submit to us online, we cannot guarantee the security of information transmitted over the internet or that unauthorized persons will not obtain access to personal information.

GPI is not responsible and has no control over websites outside its domain. We do not monitor or review the content of other parties' websites which are linked from our website or media platforms. Please be aware that we are not responsible for the privacy practices, or content of these sites. GPI will not accept any responsibility for any loss or damage in any manner, howsoever caused, resulting from your disclosure to third parties of personal information.

7. PERSONAL DATA BREACH

We have adopted procedures to deal with any suspected personal data breach and will notify you where we are legally required to do so. In the event of a notifiable breach, we will notify the relevant data protection authority as required by law (for example, within 72 hours of becoming aware of the breach where GDPR, the Nigeria Data Protection Regulation or UK GDPR applies).

8. CHILDREN

We do not intend that any portion of our online customer and vendor portals be accessed or used by persons under the age of 18, and such use is prohibited. By using the portals, you represent that you are at least 18 years old. If you are a parent or guardian of a child under the age of 18 and believe he or she has disclosed personal information to us, please contact us as indicated in **CONTACT US**. Except where prohibited by applicable law, a parent or guardian of a person under the age of 18 may review and request deletion of such person's personal information as well as prohibit the use thereof.

9. CONSENT – NIGERIA ONLY

Where the Nigeria Data Protection Regulation applies, you accept this Notice when you give consent upon access to online customer and vendor portals, or visit trade fairs, any of our offices or other venues for official or non-official purposes, or participate in any other activity online where this Notice is posted or linked or other offline activities. This Notice governs the use of our portals and services by users unless otherwise agreed through a written contract.

10. UPDATES

We may update this Notice from time to time. You will be notified in advance of any such updates. Where we are required to do so by applicable law, we will seek your consent to such changes.

11. CONTACT US

If you have any questions or comments about this Notice or the processing of your personal information, or to exercise any rights available to you under applicable law, please contact us as follows:

- 1) For the EEA, UK and Switzerland: please contact us at gdpr-privacy@graphicpkg.com;
- 2) California residents: please submit questions to California-privacy@graphicpkg.com.
- 3) For other jurisdictions: please contact us at the contact details provided [here](#).

Where permitted under applicable law, we may charge you a reasonable fee to process your request.

ADDITIONAL INFORMATION FOR CALIFORNIA RESIDENTS

This section provides representatives and personnel of our current and prospective customers, vendors' and other business partners who are California residents (“**you**”, “**your**”) with additional information under California privacy laws, notably as required by the California Consumer Privacy Act (“**CCPA**”), regarding your privacy rights, as well as our collection, use and disclosure of your personal information, as may be collected in connection with our offline business activities, online customer and vendor portals, trade fairs

and all other activities where this Notice is posted or linked. This section does not address or apply to our handling of personal information that is exempt under the CCPA.

Categories of Personal Information Collected and Disclosed. Our processing of personal information varies based upon our relationship and interactions with you, the table below identifies, generally, the categories of personal information (as defined by the CCPA) that we have collected about California residents who are representatives and personnel of our current and prospective customers, vendors’ and other business partners, as well as the categories of third parties to whom we may disclose this information for a business or commercial purpose.

| Categories of Personal Information Collected | | Categories of Third Party Disclosures |
|--|--|--|
| Identifiers | Includes direct identifiers, such as name, alias, user ID, username, account number or unique personal identifier; email address, phone number, address and other contact information; IP address and other online identifiers | <ul style="list-style-type: none"> • Affiliates and subsidiaries • Advisors and agents • Service providers • Regulators, government entities and law enforcement • Others as required by law • Internet Service Providers, operating systems and platforms |
| | Includes SSN, driver’s license number, passport number, tax ID and other government identifiers. | <ul style="list-style-type: none"> • Affiliates and subsidiaries • Advisors and agents • Service providers • Regulators, government entities and law enforcement • Others as required by law • Internet Service Providers, operating systems and platforms |
| Customer Records | Includes personal information, such as [name, account name, user ID, contact information, education and employment information, SSN and government identifiers, account number, and financial or payment information], that individuals provide us in order to purchase or obtain our products and services. For example, this may include information collected when an individual registers for an account, purchases or orders our products and services, or enters into an agreement with us related to our products and services. | <ul style="list-style-type: none"> • Affiliates and subsidiaries • Advisors and agents • Service providers • Regulators, government entities and law enforcement • Others as required by law • Internet Service Providers, operating systems and platforms |
| Commercial information | Includes records of personal property, products or services purchased, obtained, or considered, | <ul style="list-style-type: none"> • Affiliates and subsidiaries • Advisors and agents • Service providers |

| | | |
|---|---|--|
| | or other purchasing or use histories or tendencies. | <ul style="list-style-type: none"> • Regulators, government entities and law enforcement • Others as required by law • Internet Service Providers, operating systems and platforms |
| Internet and electronic network activity information | Including, but not limited to, browsing history, clickstream data, search history, and information regarding interactions with an internet website, application, or advertisement, including other usage data related to your use of any of our Services or other online services. | <ul style="list-style-type: none"> • Affiliates and subsidiaries • Advisors and agents • Service providers • Regulators, government entities and law enforcement • Others as required by law • Internet Service Providers, operating systems and platforms |
| Location data | Location information about a particular individual or device. | <ul style="list-style-type: none"> • Affiliates and subsidiaries • Advisors and agents • Service providers • Regulators, government entities and law enforcement • Others as required by law • Internet Service Providers, operating systems and platforms |
| Professional information | Includes professional and employment-related information such as current and former employer(s) and position(s), business contact information and professional memberships). | <ul style="list-style-type: none"> • Affiliates and subsidiaries • Advisors and agents • Service providers • Regulators, government entities and law enforcement • Others as required by law • Internet Service Providers, operating systems and platforms |
| Sensitive personal information | In limited circumstances, we may collect: Social security, driver’s license, state identification card, or passport number. Account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account. Precise geolocation. | <ul style="list-style-type: none"> • Affiliates and subsidiaries • Advisors and agents • Service providers • Regulators, government entities and law enforcement • Others as required by law • Internet Service Providers, operating systems and platforms |

Sales and Sharing of Personal Information. California privacy laws define a "sale" as disclosing or making available to a third-party personal information in exchange for monetary or other valuable consideration, and “sharing” broadly includes disclosing or making available personal information to a third party for purposes of cross-context behavioral advertising. We do not sell or share any personal information,

including sensitive personal information, about California residents. Nor do we sell or share any personal information about individuals who we know are under sixteen (16) years old.

Sources of Personal Information. In general, we may collect the categories of personal information identified in the table above directly from you via the forms you complete through the HICX portal. HICX may also collect personal information from you indirectly, by, for example, observing actions on their website. More information about HICX's privacy practice is available [here](#).

Purposes of Collection, Use, and Disclosure. As described in more detail in [Section 1, PERSONAL INFORMATION WE COLLECT, PURPOSES OF PROCESSING AND METHODS OF COLLECTION](#) and [Section 3, SHARING AND TRANSFERS OF PERSONAL INFORMATION](#) above, we collect, use, disclose, and otherwise process the above personal information for the following business or commercial purposes and as otherwise directed or consented to by you:

- To fulfill or meet the reason you provided the information. For example, if you share your name and contact information to ask a question about our products or services, we will use that personal information to respond to your inquiry.
- To provide you with support and to respond to your inquiries, including to investigate and address your concerns and monitor and improve our responses.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- As described to you when collecting your personal information or as otherwise permitted under the CCPA.
- For our general business and operational support. For example, to consider and implement mergers, acquisitions, reorganizations, bankruptcies, and other business transactions such as financings, and related to the administration of our general business, accounting, auditing, compliance, recordkeeping, and legal functions. Where we disclose personal information for a business purpose, we enter into a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for and purposes except performing the contract.
- For security and protection of rights. For example, to protect the services we provide and our business operations; to protect our rights or those of our stakeholders; to prevent and detect fraud, unauthorized activities and access, and other misuse; where we believe necessary to investigate, prevent or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety or legal rights of any person or third party.

Sensitive Personal Information. Notwithstanding the above, we only use and disclose sensitive personal information as reasonably necessary (i) to perform our services requested by you, (ii) to help ensure security and integrity, including to prevent, detect, and investigate security incidents, (iii) to detect, prevent and respond to malicious, fraudulent, deceptive, or illegal conduct, (iv) to verify or maintain the quality and safety of our services, (v) for compliance with our legal obligations, (vi) to our service providers who perform services on our behalf, and (vii) for purposes other than inferring characteristics about you. We do not use or disclose your sensitive personal information other than as authorized pursuant to section 7027 of the CCPA regulations (Cal. Code. Regs., tit. 11, § 7027 (2022)).

Retention. We retain the personal information we collect only as reasonably necessary for the purposes described above or otherwise disclosed to you at the time of collection. For example, we will retain your contact details for as long as necessary to complete our business transaction with you, as well as an additional period of time as necessary to protect, defend or establish our rights, defend against potential claims, and comply with legal obligations.

California Residents' Rights. Under the CCPA, California residents have the following rights (subject to certain limitations):

- **To opt out of sales and sharing.** The right to opt-out of our sale and sharing of their personal information.
- **To limit certain uses and disclosures of sensitive personal information.** The right to limit our use or disclosure of sensitive personal information to those uses authorized by the CCPA. We do not use or disclose sensitive personal information beyond the purposes permitted under the CCPA, thus this right is not available to California residents.
- **Deletion.** The right to the deletion of their personal information that we have collected, subject to certain exceptions.
- **To know/access.** The right to know what personal information we have collected about them, including the categories of personal information, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information, the categories of third parties to whom we disclose personal information, and the specific pieces of personal information we have collected about them.
- **Correction.** The right to correct inaccurate personal information that we maintain about them.
- **Non-discrimination.** The right not to be subject to discriminatory treatment for exercising their rights under the CCPA.

Submitting CCPA Requests. California residents may submit CCPA requests to access/know, correct and delete their personal information maintained by us online by submitting a request via our [webform](#), by calling us at our toll free Alertline at 1-866-898-3750, or by e-mailing California-privacy@graphicpkg.com.

We will process your request based upon the personal information in our records that is linked or reasonably linkable to the information provided in your request. In some cases, we may request additional information in order to verify your request or where necessary to process your request. If we are unable to adequately verify a request, we will notify the requestor. Authorized agents may initiate a request on behalf of another individual. Authorized agents will be required to provide proof of their authorization and we may also require that the relevant consumer directly verify their identity and the authority of the authorized agent.