Kronospan Inc. HIPAA & GDPR Privacy Statement

February 12, 2026

Policy

Kronospan Inc. and its affiliated companies are not a covered entity as defined by HIPAA; we do however maintain health care and related plans that are subject to HIPAA regulations. Because of this, Kronospan, LLC has adopted a policy that protects the confidentiality and privacy of protected health information whenever it is used by company representatives.

In addition, we are a United States–based company. While our primary operations are outside the European Economic Area (EEA), we are committed to protecting personal data and respecting the rights of individuals in the EEA in accordance with the General Data Protection Regulation (GDPR), where applicable.
This notice, as it pertains to GDPR, applies only to personal data we collect from individuals located in the EEA.

HIPAA

Definitions

- **HIPAA**: Health Insurance Portability and Accountability Act
- **PHI**: Protected Health Information
- **Affected Associates**: All Kronospan associates
- **HCO**: HIPAA Compliance Officer

Procedure

- HIPPA Regulations will be followed in the administration of health information privacy, health information security, and health information electronic transmission.
- Kronospan USA, will consider any breach of privacy and confidentiality of PHI to be serious; disciplinary action may be taken in the event a breach occurs.
- The Human Resource Director is the designated HCO and any questions or issues regarding PHI should be addressed to the HCO.
- PHI will be stored in a secured place within the HR Department
- Annually or as necessary, the company performs enrollment, changes in enrollment, and payroll deductions, provides assistance in claims problem resolution and explanation of benefits issues. Some or all of these activities may require the use or transmission of PHI. Therefore, all information related to these processes will be maintained in confidence and emp0loyees will not disclose PHI from these processes for employment-related actions, except as provided by administrative procedures approved by the HCO. In general, the following rules apply:
    - Disclosures that DO NOT qualify as PHI include: disclosure of PHI to the individual to whom the PHI belongs, requests by providers for treatment and/or payment, disclosures requested to be made to authorized parties by the individual PHI holder, disclosures to government agencies for reporting or enforcement purposes, disclosures to workers' compensation providers and those authorized by the workers' compensation providers.

    - Information regarding whether an individual is covered by a plan for claims processing purposes may be disclosed.
    - Information external to the health plan is not considered PHI if the information is being furnished for claims processing purposes involving workers' compensation and/or sort-or long-term disability and medical information received to verify ADA or FMLA status.
- Personnel record and disclosures of PHI will be maintained for a period of six years as required by federal law, unless a state law requires a longer retention period. Records that have been maintained for the maximum interval will be destroyed in a manner to ensure that such data is not compromised.

General Data Protection Regulation (GDPR)

Data Definitions

We may collect and process the following categories of personal data:

- Contact information (e.g., name, email address, phone number)
- Account or business information (if applicable)
- Technical data (e.g., IP address, browser type, device information)
- Usage data (e.g., interactions with our website or services)
- Any other information you voluntarily provide

Use of Personal Data

Personal data may be used for the following purposes:

- To provide and maintain our services
- To communicate
- To improve our website, products, and services
- To comply with legal obligations
- For legitimate business interests, where such interests are not overridden by individual rights

Legal Bases for Processing

Where GDPR applies, we rely on one or more of the following legal bases:

- Individual consent
- Performance of a contract
- Compliance with legal obligations
- Legitimate interests

Data Sharing and Transfers

We may share personal data with:

- Service providers and vendors supporting our operations
- Legal or regulatory authorities, where required

As a U.S.-based company, your data may be transferred to and processed in the United States. Where required, we implement appropriate safeguards to protect personal data.

Data Retention

We retain personal data only as long as necessary to fulfill the purposes outlined in this notice, unless a longer retention period is required or permitted by law.

Individual Rights Under GDPR

If an individual is located in the EEA, they may have the following rights:

- Right of access
- Right to rectification
- Right to erasure ("right to be forgotten")
- Right to restrict processing
- Right to data portability
- Right to object to processing
- Right to withdraw consent at any time

Individuals also have the right to lodge a complaint with a supervisory authority in their country of residence.

Data Security

Kronospan U.S. implements appropriate technical and organizational measures to protect personal data against unauthorized access, loss, or misuse.

Contact Information

Concerned parties who wish to exercise their GDPR rights, may contact the following:
Email: complianceusa@kronospanusa.com
Mailing address:
Kronospan
1 Kronospan Way
Eastaboga, Alabama, USA 36260

Updates to This Notice

We may update this GDPR Privacy Notice from time to time. Any changes will be posted on this page with an updated effective date.