Privacy Policy for the “HARTMANN Easy” Mobile App

Effective as of:

We, N.V. PAUL HARTMANN S.A., place the utmost importance on protecting your personal data. Please take the time to read this Privacy Policy carefully. This Privacy Policy provides you with information in accordance with the General Data Protection Regulation (GDPR). To fully understand this policy, it is essential to be aware of our different roles:

1. HARTMANN as the data controller (for your user data): We are the data controller for your own personal data as a user (e.g., your name, email address, and password for your user account). All sections of this policy (in particular C.1–C.4, C.7, D, E, F, G, and H) refer exclusively to this data processing, for which we are the data controller. This also expressly applies to the access to your end device described in Section D (Article 10/2 of the Belgian Data Protection Act of July 30, 2018), which concerns exclusively your device as a user (e.g., your Dienstr smartphone).
2. HARTMANN as a Data Processor (for patient data): As soon as you enter patient data in the “Care Plan” or “Wound Documentation” modules, you or your institution act as the data controller. We then act exclusively as your data processor, bound by your instructions. Sections C.5 and C.6 transparently describe our role as a data processor and the associated instructions (e.g., regarding anonymization).

Detailed provisions regarding data processing (in particular regarding your obligations as the data controller and our obligations as the data processor) can be found in the separate “Supplementary Privacy Notices” for the respective applications and in the Data Processing Agreement (DPA) that your institution enters into with us.

A. General Information and Definitions

“Personal data,” as defined by the General Data Protection Regulation (GDPR), refers to any information relating to an identified or identifiable natural person. This includes data such as your name, your email address, or your user behavior.

We strictly adhere to applicable data protection regulations and protect your data through comprehensive technical and organizational measures.

B. Data Controller and Data Protection Officer

N.V. PAUL HARTMANN S.A., Avenue Paul Hartmann, 1, 1480 SAINTES, Belgium, email: [info@hartmann.be], is responsible for processing your personal data in connection with the “HARTMANN Easy” app.

You can contact the Data Protection Officer at: N.V. PAUL HARTMANN S.A., Avenue Paul Hartmann, 1, 1480 SAINTES, Belgium, email: dataprotection.be@hartmann.info.

Data Processor: PAUL HARTMANN AG (parent company) operates this app as a central technical platform. If you use modules whose content is provided by local PAUL HARTMANN subsidiaries (e.g., the HARTMANN subsidiary in your country), PAUL HARTMANN AG processes your user data as a technical service provider (data processor) on behalf of these subsidiaries. However, we remain your central point of contact for your data protection rights regarding app usage.

C. Processing of Your Personal Data When Using the App

The scope and nature of data processing depend on how you use our app. To increase transparency on mobile devices, this statement follows the recommended “layered approach,” which allows you to navigate to the sections relevant to you by selecting the headings.

1. Downloading the App from an App Store

Certain information is processed by the app store operator as soon as you access our app listing in the respective app store (e.g., Apple App Store or Google Play Store) and when you download the app. This includes detailed statistical metrics for measuring reach (such as product page views, impressions, visitors to the store listing, and first-time downloads on a new device) as well as personal data such as your username, your email address, your account’s customer number, the time of the download, and, if applicable, payment information.

We have no influence over this data collection and processing; it is the sole responsibility of the respective app store operator (Apple or Google), which acts as an independent data controller under data protection law. We receive only aggregated, anonymized statistical reports from the store operators regarding the reach and performance of our app, which do not allow us to identify you personally. For more information on data processing in the app stores, please refer to the privacy policies of Apple or Google.

2. Technically Necessary Data Processing When Launching the App

Every time you use the app, we automatically process data that your device transmits to our servers for technical reasons. This data is absolutely necessary to ensure the stability, localization, and security of the app.

- IP address
- Date and time of the request
- Device identifier (e.g., IMEI, IMSI)
- Name of your mobile device
- Operating system and its version
- Language and version of the app

The legal basis for this processing is our legitimate interest in providing a functional and secure app in accordance with Article 6(1)(f) of the GDPR.

To ensure IT security, defend against cyberattacks (e.g., brute-force attacks on user accounts), and for technical troubleshooting (debugging), we also collect security-related log data on the server side, such as, in particular, failed registration and login attempts (Failed Registrations) in our modules. This data processing is strictly necessary to maintain system integrity and the confidentiality of your data. It is based on our legitimate interest in ensuring network and information security pursuant to Article 6(1), sentence 1, subparagraph (f) of the GDPR in conjunction with the exception provision of Article 10/2 of the Belgian Data Protection Act of July 30, 2018.

3. Registration and Management of Your User Account

Creating a user account is required to use the app. Depending on whether you are already listed as a contact with us, we distinguish between two registration methods. The data collected during this process is processed for the purpose of creating and managing your account, authenticating you, and enabling your use of the app. The legal basis for this processing is the performance of the user agreement pursuant to Article 6(1), first sentence, letter b) of the GDPR.

Specifically, the following data is processed depending on the registration method:

1. Guest Registration (for new users): As part of the registration process for new users, we collect the following required information: your title, first and last name (for unique identification and account management), your email address (as a unique identifier, for communication and login), your country (for country-specific content/regulations), the name of your institution, your ZIP code, and your industry (for assignment to the contractual partner and for B2B verification, respectively). You may optionally provide your profession. Providing your HCP/AHPRA/NPI number is also optional. The legal basis for the required information is Article 6(1)(b) of the GDPR; for country-specific mandatory information, the legal basis may additionally be derived from Article 6(1)(c) or (f) of the GDPR.

2. Contact Registration (for existing contacts): If you are already registered in our CRM system, we collect the following mandatory information for registration: your HARTMANN CRM ID (to link to your existing customer account), your first and last name (for matching and verification), your email address (as a unique identifier, for communication and login), your title (for personalized communication), and your profession (to verify your professional affiliation). The legal basis for this processing is also Article 6(1)(b) of the GDPR.

If you already have a user account for the HARTMANN Supply Management, you can use it to log in to the app. In this case, the data required for verification and linking (specifically, name, email address, and customer number) will be exchanged between the systems.

4. Data Processing for Lead Generation (the "Inco Guide" and "Wound Guide" Modules)

When registering for the free "Inco Guide" and "Wound Guide" modules, you have the option to voluntarily give us your consent to use your contact information (first name, last name, email address, job title) for marketing purposes. This consent is separate and voluntary. Use of the modules is not contingent upon granting this consent. The consent covers: - The transfer of your data to our CRM system (Salesforce) for managing prospect contacts. - Contacting you via email with information about our products, services, and events. To ensure that you actually wish to receive these emails, we use the double opt-in procedure: After you give your consent, you will receive an email with a confirmation link. You will only be added to our mailing list after clicking this link. You may revoke your consent at any time and without providing a reason, effective for the future—for example, via the unsubscribe link in every email or through your account settings in the app. Revocation does not affect the lawfulness of processing carried out up to that point . The legal basis is your explicit consent pursuant to Art. 6(1)(a) of the GDPR and Art. XII.13. § 1er of the Belgian Code of Economic Law.

5. Processing of Health Data (the "Care Plan" and "Wound Documentation" modules)

5.1. Allocation of Roles: The "Care Plan" and "Wound Documentation" modules enable you, as a healthcare professional, to process health data of third parties (patients). This constitutes special categories of personal data within the meaning of Article 9 of the GDPR. When using these modules, you (or your employer) act as the data controller under data protection law within the meaning of Article 4(7) of the GDPR. As the provider of the app, we act in this context exclusively as a data processor bound by instructions within the meaning of Article 4(8) of the GDPR, based on a data processing agreement (Article 28 of the GDPR) with your institution. Details regarding this are set forth in the Supplementary Privacy Notice.

5.2. Legal Basis for Processing as a Data Processor: We process the patient data you enter exclusively on the basis of a Data Processing Agreement (DPA) concluded with you in accordance with Article 28 of the GDPR. This agreement sets forth in detail our obligations as a service provider and ensures that processing takes place only in accordance with your instructions. Use of these modules requires the prior electronic conclusion of a Data Processing Agreement (DPA) by your administrator through electronic acceptance (click-and-wrap) with us. Use is not permitted without a DPA. Subsidiaries and parent companies may use anonymized usage data for the purposes of product improvement, research, and development. The user hereby instructs the company named in Section 12.2 of the Terms and Conditions to anonymize patient data exclusively on the basis of a legal basis to be ensured by the user (in particular, the patients' consent). Only after anonymization has been completed may this data be used by subsidiaries and/or the parent company for research, product improvement, and development.

5.3. Your Obligations as the Data Controller: As the user, you are solely responsible for ensuring a valid legal basis for your processing of patient data. This will generally be the explicit consent of the respective patient pursuant to Art. 9(2)(a) of the GDPR. It is your responsibility to obtain this consent. We, as the provider, do not obtain consent from your patients.

6. Data Processing for Anonymization

We are authorized to anonymize both technical usage data and the patient data you enter.

Anonymization of technical and general usage data: We process purely technical usage data (e.g., features used, loading times, crash reports) based on our legitimate interest pursuant to Article 6(1)(f) of the GDPR in order to anonymize this data. The anonymization process is designed to permanently and irreversibly remove any personal reference.

Anonymization of patient data: To the extent that patient data is anonymized, this is done exclusively within the scope of data processing on behalf of a client and in accordance with your instructions. The anonymized data may be used by companies belonging to the HARTMANN Group for research and development purposes.

7. Contact and Support

If you contact us via email or through a contact form, we store the data you provide (e.g., email address, name, content of the inquiry) in order to process your request. This data is deleted

as soon as storage is no longer necessary, unless there are legal retention requirements. The legal basis is

Art. 6(1)(b) or (f) of the GDPR.

D. Access to Functions on Your Device (Article 10/2 of the Belgian Data Protection Act of July 30, 2018)

In some cases, the operation of the app requires storing information on your device or accessing it. This is done in accordance with Article 10/2 of the Belgian Data Protection Act of July 30, 2018.

1. Absolutely Necessary Access (Without Consent): Certain types of access are absolutely necessary to provide the app features you have expressly requested. We do not require your consent for this. This applies to:

- Storing session information for authentication after login.
- Storing settings (e.g., language) to make the app user-friendly.

2. Access Requiring Consent: For all other access, we obtain your explicit consent before granting access. You can revoke this consent at any time in the settings of your operating system or the app. This applies in particular to:

- **Camera/photo gallery:** Only if you actively wish to take or upload a photo in the "Wound Documentation" module.
- **Analytics, tracking, and performance data (e.g., Google Firebase Analytics):** To continuously improve our app, conduct detailed analysis of user behavior, perform error analysis, and deliver targeted content, we integrate third-party tracking technologies and software development kits (SDKs), particularly Google Firebase Analytics. In this process, comprehensive interaction data (e.g., navigation paths, use of features such as the EVA chatbot or wound care guides, registration events) as well as device identifiers (e.g., mobile advertising IDs such as IDFA or GAID) are collected and analyzed.

  Since these SDKs actively store information on or access your device, the use of these analytics and marketing tools is subject exclusively to your prior, explicit, and voluntary consent via our in-app consent management tool. Withholding consent has no impact on the app's core functions.

  Detailed information on the technologies used, the scope of the metrics collected, the third-party providers involved (including data transfers to third countries), and your options for revoking consent can be found in our separate App Tracking and Analytics Policy. The legal basis for accessing the end device is Article 10/2 of the Belgian Data

Protection Act of July 30, 2018; for the subsequent processing of personal data, it is Article 6(1)(a) of the GDPR.

Refusal has no effect on the app's core functionality. The legal basis for access requiring consent is Article 10/2 of the Belgian Data Protection Act of July 30, 2018 in conjunction with Article 6(1)(a) of the GDPR.

E. Data Transfer to Third Parties and Processors

We will only disclose your data to third parties if this is permitted by law or if you have given your consent.

- **Processors:** We use carefully selected service providers (e.g., for hosting and technical maintenance) who process data on our behalf. These providers are contractually bound by our instructions in accordance with Article 28 of the GDPR and are obligated to comply with strict data protection standards. Our hosting provider is Microsoft Azure Cloud in the EU.
- **Salesforce (transfer to a third country):** As part of lead generation (see C.4.), we transfer your contact information to Salesforce, Inc., which is headquartered in the United States. This transfer is legally safeguarded by:
    1. The EU Commission's adequacy decision for the EU-U.S. Data Privacy Framework (Article 45 of the GDPR), under which Salesforce is certified.
    2. Additionally, by entering into Standard Contractual Clauses (Art. 46 GDPR) as part of our contract with Salesforce to ensure a consistently high level of protection.

We have a legitimate interest in continuously improving our products and services, ensuring the security of our app, and compiling statistical analyses of market trends. For this purpose, we process technical usage and metadata from your app usage (e.g., features used, loading times, device model, operating system version) in order to anonymize this data.

The legal basis for this processing for the purpose of anonymization is our legitimate interest pursuant to Art. 6(1)(f) of the GDPR. As part of the required balancing of interests, we have ensured that your interests worthy of protection do not outweigh ours. We use only pseudonymized data that does not allow for direct identification of you, and we take comprehensive technical measures to ensure data protection.

You have the right to object to this processing at any time on grounds relating to your particular situation (Article 21 of the GDPR).

Once the anonymization process—which is designed in accordance with the state of the art to permanently and irreversibly remove any personal reference—is complete, the anonymous data is also transferred to the parent company.

F. Retention Period

We store your personal data only for as long as is necessary to achieve the respective purposes or as required by statutory retention periods (e.g., under commercial or tax law). Once the purpose has been fulfilled or the retention periods have expired, the data is routinely deleted, provided it is no longer required for the performance or initiation of a contract. Data from your user account is deleted upon deletion of the account, subject to statutory retention obligations.

G. Your Rights as a Data Subject

You have the following rights with respect to your personal data:

- **Right of access** (Art. 15 GDPR)
- **Right to rectification** (Art. 16 GDPR)
- **Right to erasure ("right to be forgotten")** (Art. 17 GDPR)
- **Right to restriction of processing** (Art. 18 GDPR)
- **Right to object to processing** (Art. 21 GDPR), provided that the processing is based on Art. 6(1)(f) GDPR.
- **Right to data portability** (Art. 20 GDPR)
- **Right to withdraw consent** (Art. 7(3) of the GDPR) with future effect.
- **Right to lodge a complaint with a data protection supervisory authority** (Art. 77 GDPR)

To exercise your rights, you may contact us or our Data Protection Officer at any time.

H. Data Security

We implement comprehensive state-of-the-art technical and organizational security measures (TOMs) to protect your data against accidental or intentional manipulation, loss, destruction, or access by unauthorized persons.

I. Changes to This Privacy Policy

We are constantly developing our app. Therefore, we reserve the right to amend this Privacy Policy as needed. The current version is available within the app at any time.