Data Processing Agreement
For Dermicus Connected Services

This Data Processing Agreement ("**DPA**") applies in respect of Dermicus' Connected Service (if any) You operate.

WHEREAS users are entitled to use identified products and/or services provided by or connected with Dermicus' solutions over the cloud (the "**Connected Services**") pursuant to the license entitlement granted by Dermicus to the entity ("**End User**") permitting You to access the Connected Services;

WHEREAS in rendering the Connected Services, Dermicus (acting as Data Processor) may from time to time be provided with, or have access to information of individuals who are permitted to use the Connected Services and this information may qualify as personal data within the meaning of the GDPR;

WHEREAS End User (acting as Data Controller) engages Dermicus as a commissioned processor acting on behalf of End User as stipulated in art. 28 GDPR;

WHEREAS European data protection laws require data controllers in EU/EEA countries to provide adequate protection for transfers of personal data to non-EU/EEA countries and such protection can be achieved by requiring processors to enter into the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries ("**EC Standard Contractual Clauses**") pursuant to Commission Decision 2010/87/EU of 5 February 2010 as set out in appendix III;

WHEREAS this DPA contains the terms and conditions applicable to the processing of such personal data by Data Processor as a commissioned data processor of Data Controller with the aim to ensure that the Parties comply with the Applicable Data Protection Laws.

1. Definitions

For the purpose of this DPA, the terminology and definitions as used in the GDPR shall apply. In addition to that,

"Affiliate" means any of Affiliate(s) of End User which (a) is subject to the data protection laws and regulations of the EEA , and (b) is permitted to use the Connected Services.

"Applicable Data Processor law" means the Data Protection Laws that are applicable to Dermicus as the Data Processor.

"Applicable Data Protection Law" means the Data Protection Laws applicable to the Data Controller.

"Dermicus" means Dermicus AB, with registered office at Kungsgatan 4, 411 19 Göteborg Sweden and its subsidiaries.

"Data Controller" is a reference to End User.

"Data Importer" means the Data Processor or Sub-Processor that is located in a Third Country.

"Data Exporter" means the Data Controller if (a) (i) the Data Controller is located in the EEA or (ii) is located outside of the EEA and is subject to GDPR, and (b) Data Controller transfers personal data to a Data Importer.

"Data Processor" is a reference to Dermicus.

"**Data Protection Law**" means the GDPR and the laws and regulations containing rules for the protection of Data Subjects with regard to the Processing, including without limitation security requirements for and the free movement of Personal Data, implementing or completing the GDPR.

"**EC Standard Contractual Clauses**" means the European Union standard contractual clauses for international transfers from the European Economic Area to third countries, for the time being the clauses attached hereto as Appendix III by reference pursuant to the European Commission's decision (EU) 2021/914 of 4 June 2021 or any subsequent version issued pursuant to article 46(2) GDPR.

"**EEA**" means all member states of the European Union (excluding the United Kingdom), Norway, Iceland, Liechtenstein and, for the purposes of this DPA, Switzerland.

"Employee" means any employee, agent, contractor, work-for-hire or any other person working under the direct authority of Dermicus. However, "Employees" do not include "Sub-Processors".

"End User" is the person or entity on whose behalf this DPA is accepted.

"End User Data" means Personal Data for which End User is the Data Controller under Applicable Data Protection law, which are being shared with Dermicus in the provision of the Connected Services.

"GDPR" means regulation 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
"Non-Adequate Country" means a country that is deemed not to provide an adequate level of protection of Personal Data within the meaning of the articles 44-45 GDPR.
"Sub-Processor" means any Processor engaged by Dermicus that Processes End User Data.
"Third Country" means those countries that are not member states of the EU or the EEA (as defined herein).
"Third Party" means any party other than Dermicus, Sub-Processor or End User.

2. Instructions
2.1 To the extent Dermicus Processes End User Data required for the provision of the Connected Services it shall act as a Data Processor on behalf of End User, being the Data Controller.
2.2 End User is obliged to ensure that any instruction given to Dermicus is in compliance with Applicable Data Protection Law.
2.3 In the provision of the Connected Services, Dermicus shall Process the End User Data only on documented instructions from Data Controller unless Dermicus is required to Process End User Data by Union or by a Member State law to which Dermicus is subject; in such case, Dermicus shall inform the End User of that legal requirement before Processing, unless that law prohibits such information -.
2.4 This DPA are Data Controller's complete and final instructions to Dermicus with regard to the Processing.
2.5 Appendix I to this DPA sets out certain information regarding the Processing of the End User Data as required by article 28 of the GDPR (and possibly, equivalent requirements of other Data Protection Laws).
2.6 If Dermicus believes that an instruction of Data Controller infringes the Applicable Data Processor Law, Dermicus shall promptly inform Data Controller.
2.7 Any further instructions that go beyond the instructions contained in this DPA must be within the subject matter of this DPA. If the implementation of such further instructions results in costs for Dermicus, Dermicus shall inform Data Controller about an estimation and reasoning of such costs before implementing the instruction. Data Controller shall give further instructions generally in writing, unless the urgency or other specific circumstances require another form. Instructions in another form shall be promptly confirmed in writing by Data Controller.

3. Applicable law
3.1 When performing this DPA, Data Controller shall comply with the Applicable Data Protection Law and Dermicus shall comply with the Applicable Data Processor Law.
3.2 Each party shall deal with reasonable requests for assistance of the other party (including of End User) to ensure that the Processing complies with Applicable Data Protection Law.

4. Obligations of Data Controller
4.1 Data Controller warrants that Data Controller Personal Data is lawfully obtained from Data Subject and is lawfully provided to Dermicus under the Applicable Data Protection Law.
4.2. Data Controller further warrants that
i) it provides Dermicus with Personal Data that is up-to-date and relevant for the Processing activities;
ii) it has provided Data Subject all necessary and relevant information with regard to the Processing of the Personal Data as required under the Applicable Data Protection Law; and
iii) the End User Data does not infringe any third-party rights.
4.3. Data Controller agrees that it remains the contact point for Data Subject and that it will inform Data Subject about this. Should a Data Subject contact Dermicus with regard to correction or deletion of its Personal Data, Dermicus will use commercially reasonable efforts to forward such requests to End User.

5. Obligations of Dermicus
5.1 Security. Dermicus shall implement appropriate technical, physical and organisational security measures as specified in Appendix II taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons to ensure a level of security appropriate to the risk and to protect End User Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all other forms of unlawful Processing including, but not limited to, unnecessary collection or further Processing.

5.2 Non-disclosure and confidentiality. Dermicus shall keep End User Data confidential and shall not disclose End User Data in any way to any Employee or Third Party without the prior approval of Data Controller, except where, (i) subject to this Section, the Disclosure is required for the performance of the Processing, or (ii) subject to Section 8.1 ii), where End User Data need to be disclosed to a competent public authority to comply with a legal obligation or as required for audit purposes. Dermicus shall provide the Employees access to End User Data only to the extent necessary to perform the Processing. Dermicus shall ensure that any Employee it authorizes to have access to End User Data Processed on behalf of End User has committed himself to confidentiality or is under an appropriate obligation of confidentiality.

6. Sub-Processors

6.1 Data Controller agrees that Dermicus may use Sub-Processors to fulfill its contractual obligations under this DPA or to provide certain services on its behalf, such as providing support services or hosting services. Dermicus currently engaged Amazon Web Services Inc. as Sub-Processor to carry out Processing activities on End User Data on behalf of End User (eu-central-1, **Europe (Frankfurt)** and eu-west-2, **Europe (London)** https://aws.amazon.com/about-aws/global-infrastructure/).

6.2 Dermicus shall inform the Data Controller of any intended changes concerning the addition or replacement of Sub-Processors via Dermicus' usual email notification process. Data Controller shall not unreasonably object to such changes.

6.3 Where Dermicus subcontracts (part of) the Processing of End User Data on behalf of End User, it shall do so only by way of a written agreement with the Sub-Processor which imposes the same or essentially the same data protection obligations on the Sub-Processor as are imposed onto Dermicus under this DPA. Dermicus remains liable for the Sub-Processor's breach of its data protection obligations under such written agreement.

7. Audit and compliance

7.1 Dermicus shall, upon reasonable notice (no less than two (2) months) and not more than once every two years (unless there is a Personal Data Breach), allow its procedure and documentation to be inspected or audited by Data Controller (or the auditor of its choice, excluding any Dermicus competitor) during business hours in order to ascertain compliance with the obligations set forth in this DPA, in which case Dermicus shall make the processing systems, facilities and supporting documentation relevant to the Processing of End User Data available for an audit by End User. For the avoidance of doubt, the scope of such audit shall be limited to documents and records allowing the verification of Dermicus' compliance with the obligations set forth in this DPA and shall not include financial documents or records of Dermicus or any documents or records concerning other customers of Dermicus.

8. Notifications of Disclosures and Personal Data Breaches

8.1 Dermicus shall use reasonable efforts to inform Data Controller as soon as reasonably possible if:

i) it receives an inquiry, a subpoena or a request for inspection or audit from a competent public authority relating to the Processing, except where Dermicus is otherwise prohibited by law from making such disclosure;
ii) it intends to disclose Personal Data to any competent public authority; or
iii) it becomes aware of a Personal Data Breach.

8.2 In the event of a Personal Data Breach, Dermicus shall take reasonable remedial measures to preserve the confidentiality of the End User Data. Furthermore, Dermicus shall provide Data Controller the information reasonably requested by End User regarding the Personal Data Breach. This information will at least contain the following elements:

i) a description of the nature of the Personal Data Breach, including the number and categories of Data Subject and personal data records affected;
ii) a description of the likely consequences of the Personal Data Breach; and
iii) a description how Dermicus proposes to address the Personal Data Breach, including any mitigation efforts.

8.3 Data Controller agrees that an Unsuccessful Security Incident will not be subject to this Section 8. An "Unsuccessful Security Incident" is one that results in unauthorised access to End User Data or to any of Dermicus' or Sub-Processor's equipment or facilities storing End User Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorised access to traffic data where it can be reasonably concluded that such access did not result in access beyond headers) or similar incidents where it can be reasonably concluded that such access did not result in an actual destruction, loss, alteration or unauthorised disclosure of Personal Data.

8.4. Dermicus' obligation to report or respond to a Personal Data Breach under this Section 8 is not and will not be construed as an acknowledgement by Dermicus and any of Dermicus' subprocessors of any fault or liability of Dermicus with respect to the alleged Personal Data Breach.

9. Cooperation and assistance duty

9.1 Dermicus will reasonably assist Data Controller in the fulfilment of its obligation to respond to requests from Data Subjects, provided that (i) Data Controller has instructed Dermicus to do so by way of a written instruction and (ii) Data Controller reimburses Dermicus for the costs arising from this assistance.

9.2 Dermicus shall promptly inform Data Controller of any complaints, requests or enquiries received from a Data Subject, including but not limited to requests to rectify or erase End User Data or to object to the Processing of End User Data. Dermicus shall not respond directly to any complaints, requests or enquiries received from Data Subject without Data Controller's prior written instruction, except where required by law.

9.4 Upon written request of Data Controller, and subject to the provisions of clause 7.1., Dermicus shall make available to Data Controller all information necessary to demonstrate compliance with the Applicable Data Protection Law.

9.5 Upon written request of Data Controller, Dermicus shall, taking into account the nature of the Processing and the information at its disposal, assist Data Controller in ensuring compliance with the obligations regarding security of the Processing, notification of Personal Data Breaches and mandatory data protection impact assessments (articles 32-36 GDPR).

9.6 Dermicus shall cooperate with the supervisory authorities in the performance of their duties.

10. Return and destruction of Personal Data

Upon termination of the provision of the Connected Services, Dermicus shall – at a reasonable fee - , at the option of Data Controller expressed in writing, return and/or delete the End User Data and copies thereof to Data Controller, except to the extent applicable law provides otherwise. In that case, Dermicus shall no longer Process the End User Data, except to the extent required by applicable law.

11. Affiliates

11.1 The parties acknowledge and agree that, by using the Connected Services, the End User enters into the DPA for its own account and, as applicable, in the name and on behalf of its or their Affiliates. End User and each Affiliate agree to be bound by the obligations under this DPA. All access to and use of the Connected Services by Affiliates must comply with the terms and conditions of the DPA and any violation of the terms and conditions of this DPA by an Affiliate shall be deemed a violation by End User.

11.2 End User shall remain responsible for coordinating all communication with Dermicus under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of End User and any relevant Affiliates.

12. Liability

12.1 Dermicus indemnifies Data Controller for all claims, losses or damages incurred by Data Controller and arising directly out of a breach by Dermicus of this DPA and/or the Applicable Data Processing Law provisions directed to Dermicus, unless Dermicus proves that it is not responsible for the event giving rise to the liability.

12.2 Data Controller indemnifies Dermicus and holds Dermicus harmless against all claims, losses or damages incurred by Dermicus and arising directly out of a breach of this DPA and/or the Applicable Data Protection Law by End User.

12.3 Each party's liability will be limited to foreseeable, direct and personal damage suffered, excluding indirect, incidental, special or consequential damage and regulatory fines, even if advised of the possibility thereof. Indirect Damage shall mean damage or loss that do not directly and immediately result from an event giving rise to the liability, including but not limited to loss of earnings, business interruption, increase of personnel cost, failure to realize anticipated savings or benefits.

12.4 In any event and to the extent permitted by law, Dermicus' aggregated maximum liability under this DPA will be limited to the amounts received for the provision of the Connected Services in the twelve months preceding the incident giving rise to liability.

13. Data transfer

13.1 Dermicus shall not transfer End User Data to any Non-Adequate Country outside the EEA or make any End User Data accessible from any such Non-Adequate Country without adequate protection.
13.2 Any transfer of Personal Data to a Non-Adequate Country shall be governed by the terms of the EC Standard Contractual Clauses (Appendix III) or other model clauses that have been approved by the EU commission or another competent public authority in accordance with the Applicable Data Processing Law. Dermicus shall conclude these clauses on behalf of Data Controller. The Appendices of these clauses will contain the same or essentially the same information as this DPA. Dermicus and Data Controller shall work together to apply for and obtain any permit, authorization or consent that may be required under Applicable Data Processing Law in respect of the implementation of this Section.

14. Annexes
The following Annexes are attached hereto and made a part hereof:

Appendix I: Details of processing
Appendix II: Technical and organisational measures
Appendix III: EC Standard Contractual Clauses

15. Signatures

YOU HEREBY ACKNOWLEDGE TO HAVE READ, UNDERSTOOD AND ACCEPTED TO BE BOUND BY ALL THE TERMS AND CONDITIONS OF THIS DATA PROCESSING AGREEMENT AS INDICATED ABOVE AND IN APENDIX

_____

_____

Appendix I
Details of Processing

This Appendix 1 includes certain details of the Processing of End User Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of End User Data
The subject matter of the Processing of the End User Data is to allow Dermicus to provide its purpose-built skin solutions to the End User for use within its business and for providing health care to its customers, as set out in this DPA.
End User Data will be Processed for the duration of the provision of Connected Services for the benefit of the End User.
End User Data can be Processed outside the EEA by Sub-Processors. For transfers of personal data outside the EEA Dermicus relies on the standard contractual clauses approved by the European Commission.

The nature and purpose of the Processing of End User Data
Dermicus is managing the hosting environment on behalf of the Data Controller to enable the provision of the Connected Services.

In addition to Dermicus acting as a data processor, Dermicus also processes personal data on its own initiative for the purposes explained below, without receiving instructions from the End User. With regard to these processing activities, Dermicus itself is responsible for processing, and therefore data controller next to the processing activities by the End User. Dermicus only processes the personal data related to the provision of services in the following limited cases:

- In order to activate/use the service
  Dermicus collects information about the individual user and his organisation as it is entered in the Dermicus applications. For this purpose, Dermicus processes contact data such as name, email address, address and phone number as well as organisational data such as healthcare organisation, healthcare center, user role and job description.
  The data is processed on the basis of the performance of a contract.
- In order to provide support
  The Dermicus applications automatically collect usability data such as user activity logs, error reports, environmental data (type of browser, operating system, etc.). This is required to be able to provide the necessary support and troubleshooting to the individual users.
  The data is processed on the basis of the performance of a contract.
- In order to optimize subscription and usage
  The Dermicus applications automatically collect usability data such as user activity logs, error reports, environmental data (type of browser, operating system, etc.) and database statistics on organisation, center and/or user level (number of patients, number of cases per product, etc.). This is required to offer information on the subscription status and usage, for invoicing purposes for pay-per-use subscriptions, to provide usage recommendations to optimize the subscription and to allow the user to make optimal use of the Dermicus functionalities.
  The data is processed on the basis of the performance of a contract.
- In order to improve the product
  The Dermicus applications automatically collect usability data on an aggregated level such as user activity logs, error reports, environmental data (type of browser, operating system, etc.), and database statistics on an aggregated level (number of patients, number of cases per product, etc.). This is required for Dermicus to continuously improve the performance of the Dermicus solutions and to provide analytics (e.g., user experience, feature set and functionality, performance of algorithms, etc.).
  The data is processed on the basis of Dermicus' legitimate interest to continually improve its products.

The types of End User Data to be Processed
- User data
  - User identification data: user name, IP address, HSA-ID
  - User contact details: name, email address, phone number, address
  - User organisational data: healthcare organisation, healthcare center, user role, job description, user groups
  - User preferences (settings)
  - Usability data: user activity logs, error reports, environmental data (type of browser, operating system, etc.)

    - User email notifications
    - User chat messages: private and group chat messages
- Patient data
    - Patient identification data: name, date of birth, gender, patient ID / social security number
    - Patient contact details: phone number, address
    - Patient consent data
    - Patient health data: patient risk information, patient history, patient images, lesion or wound characteristics and risk information, diagnosis, management/treatment, notes, conclusion and reports of consultations
    - Analysis data: the outcomes of applying image analysis, post-processing and algorithms on the patient data

The categories of Data Subjects to whom the End User Data relates

- End User's employees (including End User's agents, advisors, freelancers and consultants) and End User's representatives (who are natural persons)
- Customers of the End User, its employees and representatives
- Customers of the End User's customers, its employees and representatives
- Users of the Dermicus Product authorized by the End User to use the products

Appendix II
Technical and organisational measures

1. ***The pseudonymisation and encryption of personal data; (art. 32, par. 1, lit. a, GDPR)***
    a. based on a risk assessment Dermicus will ensure a level of security appropriate to the risk, including inter alia as appropriate:
        i. Pseudonymization
        ii. Encryption, conform Cryptographic Controls policy

2. ***Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (art. 32, par. 1, lit. b, GDPR)***
    a. Dermicus is verified under ISO/IEC 27001:2013 covering the business processes, infrastructure and tools related to software development, sales, deployment, and support of our Dermicus product line in our Swedish location.
    b. Security and privacy by design
    c. Compliance with the security policies in place at Dermicus, covering
        i. Information Security Top Policy
        ii. Code of Digital Conduct
        iii. Acceptable Use
        iv. Logical Access Control
        v. Third Party Security
        vi. Backup and Recovery
        vii. Password
        viii. Info Sec Incident Management
        ix. Anti Malware
        x. Network Protection
        xi. Cryptographic Controls
        xii. IT Operations
        xiii. Cloud Security
        xiv. Secure SDLC
        xv. Disposal and Destruction
        xvi. Physical Environmental Security
        xvii. Secure Remote Support Policy

3. ***The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (art. 32, par. 1, lit. c, GDPR)***
    Compliance with the security policies in place at Dermicus, covering
        i. Backup and Recovery
        ii. IT Operations

4. ***Process for regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the data processing (art. 32, par. 1, lit. d, GDPR)***
    a. Product Security Incident Response teams (psirt): https://Dermicus.atlassian.net/servicedesk/customer/portals
    b. Dermicus operates in three lines of defense, covering operations, governance and internal audit.
    c. Regular evaluations by independent third parties (e.g. penetration testing, audit, …)
    d. Integration of automated security scanning tools during the development process (Secure SDLC) and operations

Appendix III
EC Standard Contractual Clauses

The 2021 Standard Contractual Clauses[1] are incorporated into the DPA by reference, and will apply in the following manner:

Module Two (Controller to Processor) will apply where End User is a controller of Personal Data and Dermicus is a processor of Personal Data.

For this Module:

i) Clause 7 will not apply;
ii) in Clause 9(a), Option 2 will apply, and the time period for prior notice of Sub-Processor changes will be as set forth in Section 6 of the DPA;
iii) in Clause 11(a), the optional language will not apply;
iv) in Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by the laws of Sweden;
v) in Clause 18(b), disputes will be resolved by the courts of Sweden;
vi) Annex I.A (List of parties)
The End User (as defined under Section 1 of the DPA) acts as data exporter and Dermicus (as defined under Section 1 of the DPA), on behalf of Dermicus' (Sub-)Processors located in a Third Country, acts as data importer for the construction of these 2021 Standard Contractual Clauses. Further contact details are part of the DPA and Appendix I.
vii) Annex I.B (Description of Transfer)
The Parties agree that Appendix I to the DPA (as well as Section of DPA in respect of transfers to (sub-processors) describe the transfer as required under the 2021 Standard Contractual Clauses.
viii) Annex I.C (Competent Supervisory Authority)
The competent supervisory authority is the supervisory authority that has primary jurisdiction over the data exporter.
ix) Annex II (Technical and Organisational Measures – Security of the Data)
Described in Appendix II to the DPA
x) Annex III (List of Sub-processors)
The Data Controller has authorised the use of the sub-processors as mentioned in Section 6.1 of this DPA

1 Annex to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, or any subsequent version issued pursuant to article 46(2) GDRP