



PRIVACY POLICY

The privacy policy is effective as of 2024-11-15

1 PURPOSE

- 1.1 Personal data refers to any information that directly or indirectly can be attributed to a living individual (**"Personal Data"**). This policy describes how personal data and information about you may be used and disclosed and how you can obtain access to this information when using our services.

2 INTRODUCTION

- 2.1 We at Evira, ("**Evira**", "**we**" or "**us**" as defined in section 5, "Legal entity and contact details") value your privacy and are committed to keeping your data confidential.
- 2.2 We provide a website (the "**Website**") with public information about our services, the Evira mobile application for treatment of patients with obesity (the "**App**"), and a care portal for use by healthcare professionals (the "**Care Portal**"). Evira is the data controller for the processing of the personal data that we receive when you use the Website or the App and is therefore responsible for ensuring that all personal data is processed correctly and in accordance with applicable data protection regulations. The Website, App and Care Portal are jointly referred to ("**Services**").
- 2.3 Evira does not provide medical services. When you seek care from any healthcare provider that offers Evira treatment, the healthcare provider provides medical services to you (the "**Healthcare provider**"), it is the Healthcare provider who is the data controller for the processing of personal data that takes place for the purpose of providing you with the services that the Healthcare Provider offers inside the Evira care portal, e.g. various types of healthcare services. In relation to these Healthcare Providers, Evira is the data processor regarding the processing of personal data to, for example, provide the operation of the Services.
- 2.3.1 Sensitive personal data are data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, and personal data concerning health or sexual life ("**Sensitive Personal Data**"). Health data may for example be health conditions, doctor's appointments and treatments.



- 2.3.2 Evira only processes Sensitive Personal Data as a data processor in relation to the Healthcare Provider, who is the data controller for such Sensitive Personal Data. Therefore, it is the Healthcare Provider that processes, for example, patient data and health information for the purpose of providing healthcare through the Service and other necessary treatment or advice within the framework of the Healthcare Provider's exercise of care.
- 2.3.3 The Healthcare Provider is obligated to process Personal Data and Sensitive Personal Data in accordance with relevant data protection and patient data legislation. The Healthcare Provider instructs Evira to process Personal Data and Sensitive Personal Data for the purpose of providing the Service.
- 2.3.4 Collected information about the User's physical health condition may be analysed together with any additional information recorded through forms or from clinic personnel to create a more comprehensive view of the User's health condition. This could, for example, involve risk assessments for development of various related diseases or an assessment of which interventions are most likely to lead to long-term sustainable results. This processing may be performed by Evira on behalf of the Healthcare Provider and thus in accordance with the Healthcare Provider's instructions given to Evira.
- 2.4 This privacy policy (the "**Privacy Policy**") describes how we collect, process and protect personal data when you as a User visit the Website, use the App or Care Portal, as well as the rights that pertain to you when we process your personal data.
- 2.5 If you have questions regarding our processing of your personal data, it is always possible to contact us. Information about us and our contact details can be found under section 5, "**Legal entities and contact details**", below.

3 SCOPE OF THE PRIVACY POLICY

- 3.1 The Privacy Policy covers the processing of personal data for which Evira is the data controller. The Privacy Policy thus does not cover the processing of personal data that Evira carries out as a data processor, i.e., on behalf of the Healthcare Provider. Evira is then bound by the instructions for personal data processing that Evira has received from the Healthcare Provider. In these situations, Evira will always ensure that processing takes place in accordance with applicable data protection regulations and as far as possible in accordance with this Privacy Policy.
- 3.2 This Privacy Policy applies to persons using our Services, i.e. persons visiting the Website or who are users of the App or Care Portal ("**Users**").



3.3 The App may contain links to other sites that are not operated by Evira. If you click a third-party link, you will be directed to that third party's website or service. We strongly advise you to review every link you visit for applicable privacy policies. Evira has no control over and assumes no responsibility of third party links or services. This Privacy Policy does not apply to your use or access of third party services.

4 Agreement to Privacy Policy terms

4.1 By accessing and/or using the Services, you are acknowledging that you have read and agree to the terms of this Privacy Policy. If you do not agree, Evira cannot deliver the Services, and you must immediately cease using the Services.

5 Legal entity and contact details

5.1 For questions regarding Evira's Privacy Policy or regarding Evira's processing of Personal Data, contact:

Depending on where you are using our Services the following legal entities apply:

EU: Evira AB, org. nr. 559252-8995

UK: Evira Ltd, company nr. 15159570

Data Protection Officer: dataprotection@evira.se

Visiting address:
Triewaldsgränd 2
111 29 Stockholm
Sweden

Postal address:
Evira AB
Triewaldsgränd 2
111 29 Stockholm
Sweden

Email: info@evira.se

6 Updates to the Privacy Policy



- 6.1 Evira reserves the right to revise the Privacy Policy. The date of the latest change is stated at the beginning of the Privacy Policy. If Evira introduces material changes to the Privacy Policy, we will publish these changes on: <https://www.evira.se/en/privacy-policy>. The User is recommended to regularly read the Privacy Policy to be aware of any changes.
- 6.2 We will notify you of significant changes by electronic means. If you do not agree with the changes, you should stop using the Services immediately. If you continue to use the Services, you will agree to the new changes and you will be bound by the updated Privacy Policy terms.

7 Language of the Privacy Policy

- 7.1 The Privacy Policy is available in English and other languages. For other languages, we use machine translation from English. Machine translations may not yield perfect results, so in cases of dispute over the interpretation, the source language of English shall prevail. Please note that no potential disputes over provisions will be interpreted to the detriment of the consumer within the meaning of the law.

8 GENERAL INFORMATION ABOUT PERSONAL DATA THAT IS PROCESSED IN THE SERVICES

- 8.1 For transparency, we present a summary with respect to which Personal Data Evira processes in the form of data controller and data processor. A detailed description of the different data type categories follows in chapter 9.

| Data category | Evira | Healthcare Provider (HP) | Legal basis |
|------------------|-----------------|--------------------------|------------------|
| Integration data | Data processor | Data controller | HP's instruction |
| Demographic data | Data processor | Data controller | HP's instruction |
| Medical data | Data processor | Data controller | HP's instruction |
| Website data | Data controller | - | 6.1.f GDPR |
| Obligated data | Data controller | - | 6.1.c GDPR |
| Account data | Data controller | - | 6.1.f GDPR |
| Support data | Data controller | - | 6.1.f GDPR |
| Services data | Data controller | - | 6.1.f GDPR |
| Information data | Data controller | - | 6.1.a GDPR |



9 **Categories of Personal data that is processed in the Services**

We process different categories of personal data from you. Each category of data is explained below:



9.1 **Integration data:** We may process data that you provide to us through integrations with our Services (e.g. Apple Health or similar). For example, if you allow, we can track your daily step counts in the App and to the Healthcare Provider.

Evira processes this data based on instructions in a data processing agreement with the data controller according to Article 28 GDPR.

You can turn this data collection on inside the App. If you choose to do so, this data is collected in the App and provided towards the Healthcare Provider.

9.2 **Demographic data:** We may process demographic data which may include, but is not limited to, your name, phone number and email address. The collection of this demographic data is primarily used to provision the Services towards App users and Care Portal users.

Evira processes this data based on instructions in a data processing agreement with the data controller according to Article 28 GDPR.

9.3 **Medical data:** We may process information regarding your health conditions, including, but not limited to, age, gender, weight, height, medical history, symptoms and communication between patients and Healthcare Providers. We collect this information to provide you with the Services and to provide the Healthcare Provider with the information required to provide medical treatment through the Services.

Evira processes this data based on instructions in a data processing agreement with the data controller according to Article 28 GDPR.

9.4 **Website data:** When you visit our Website we may process information about how you access the Website, which also includes information about operating systems, IP address, network identifiers, and website data. Personal data is processed so that we can improve the user experience and analyse the user of the Website. Please refer to our Cookie Policy to understand how we work with Cookies.

Legal basis for processing by Evira is Article 6.1.f of the GDPR. The legitimate interest lies in analysing the use of the Website and developing it further.

9.5 **Account data:** If you create an account in the Services, we may collect your email address and telephone number and technical or other information from you through the Services. Such information will be used for the purposes of



provisioning your account in the Services and will enable you to log in and customise settings towards the Services.

Legal basis for processing by Evira is Article 6.1.f of the GDPR. The legitimate interest lies in providing you with access to the Services, but also to communicate to you about news and updates to the Services.

Data is obtained directly from you when you create your account in the Services. The data is processed from the moment you create your Account to the moment you delete your Account.

- 9.6 **Support data:** If you are in contact with us for support or to lodge a complaint, we may collect technical, troubleshooting or other information from you through log files and other technologies, some of which may qualify as Personal Data (e.g. IP address). Such information will be used for the purpose of troubleshooting and technical support in accordance with this Privacy Policy.

Legal basis for processing by Evira is Article 6.1.f of the GDPR. The legitimate interest lies in providing you with assistance when using the Service, but also for the purpose of further enhancing the Services.

Data is obtained directly from you or in connection with your actions in the Services. We will never ask for your login credentials, financial or medical information. Never provide such information outside of the Services.

From the moment you are in contact with us regarding a support matter until the issue is resolved the primary purpose of the data processing is to provide you with support. After the issue is resolved or archived, the data is processed for secondary archiving purposes. The secondary purposes are verifying the quality of the Services provided to you, and for investigating, establishing or resolving legal claims. After account deletion, we process this information up to 24 months for these purposes. The recipients of this data can only be authorised employees or contractors who provide services to us working under strict confidentiality.

- 9.7 **Services data:** When you use the Services, we may process Services data including, but not limited to, your IP address, device information, location, browser type, internet service provider, system configuration information, date and time stamps of your actions in the Services. This information is used to provide the Services to you, analyse overall Services usage trends, help resolve technical issues and improve the Services over time. Without this data we cannot fulfil our commitments, and we cannot provide the Services.



We do not monitor activity for specific users of the Services, except for technical support as described above. Services data is based on statistical patterns which does not rely on individual User's activities.

Legal basis for processing by Evira is Article 6.1.f of the GDPR. The legitimate interest lies in processing data that contains logs that can later be used to provide technical support, inform decisions on Services design and software development.

Data is obtained directly from you when you use the Services. The data is processed during the time we provide the Services to you and for a period of 36 months thereafter to be able to handle any claims and warranty issues.

- 9.8 **Obligated data:** We also process Personal Data to fulfil our legal obligations when providing the Service. This includes processing that is necessary to be able to fulfil our legal obligations according to legal requirements, judgments or authority decisions (for example accounting laws).

Legal basis for processing by Evira is Article 6.1.c of the GDPR. We may store the Personal Data for this purpose for a period of up to 7 years.

- 9.9 **Information data:** We may collect your email address, name and other relevant contact details to send you general news, updates, and information about Evira, including new features, services, or events we think may interest you.

Legal basis for processing by Evira is Article 6.1.a of the GDPR, i.e. your consent. You have the right to withdraw your consent at any time, which you can do by altering your account settings, or clicking an unsubscribe link provided in our communications.

- 9.9.1 **Statistical data:** Evira processes aggregate data of the Services by Users. This data does not constitute Personal Data because it is anonymised, meaning we do not process any data that could link the readings we collect with you or any other User. This data enables us to do analysis, and on this basis, we create statistics that allow us to group information and use it for various purposes such as Services development, materials, and publications.

10 **RECIPIENTS OF PERSONAL DATA AND TRANSFER OUTSIDE OF THE EU/EEA**

- 10.1 Evira uses IT providers within the EU/EEA for the operation of the Service and storage of Personal Data. When transferring Personal Data to a third country (i.e. a country outside the EU/EEA), Evira takes appropriate measures to ensure that the transfer takes place in accordance with applicable data protection legislation. This



includes approved transfer mechanisms according to Chapter V GDPR such as standard data protection clauses, decisions on adequate levels of protection, and additional protective measures.

11 RIGHTS AS A REGISTERED USER

11.1 As a User you have the right to:

- (i) request information about which personal data we process about you and request a copy of these (*extract from the register*);
- (ii) have incorrect personal data corrected and, in some cases ask us to delete Personal Data;
- (iii) object to certain personal data being processed and request that the processing of personal data is limited;
- (iv) have the personal data you have provided to us transferred to another data controller (*right to data portability*); and
- (v) if you are dissatisfied with how we process your personal data, you can file a complaint with the relevant supervisory authority for data inspection.

11.2 Users can retrieve, delete or limit the processing of personal data by sending a support message in the Service. Please note that if a User requests that we limit the processing of or delete the User's Personal Data, it may mean that we will not be able to provide the Service.

12 SECURITY

12.1 Evira has taken appropriate technical and organisational measures to protect Personal Data against loss, misuse, unauthorised access, disclosure, alteration, and destruction. To ensure that Personal Data is processed in a secure and confidential manner, we use industry-standard technologies, including TLS and token-based authorisation, to limit access to data and protect against intrusion. All access to administrative and clinic accounts with access to user data requires authentication with two factors (BankID or equivalent solutions). For more information regarding Evira's security measures when processing Personal Data, please refer to Evira's information security standards policy.

12.2 Since access to Personal Data is given after logging in, it is important that Users choose a secure password so that no one else can access the information. Since the email address is used for communication, it is important that the User



protects it with a secure password and promptly informs us if the User loses control over it.

13 NATIONAL DATA OPT-OUT COMPLIANCE

- 13.1 The National Data Opt-Out allows patients that get treatment within the NHS to choose to prevent their confidential patient information from being used for purposes other than their individual care. This opt-out respects our patients' wishes and ensures that their privacy is upheld to the highest standard.
- 13.2 Evira fully respects and complies with the National Data Opt-Out policy. We have systems in place to ensure that patient data is not used or disclosed in a way that would contradict the opt-out. If any use or disclosure of data needs to adhere to the opt-out, we remove records for patients who have chosen this preference.
- 13.3 Our processes related to the National Data Opt-Out are regularly reviewed to ensure continued compliance and respect for our patients' preferences. Our Data Security and Protection Toolkit assessment confirms our adherence to the policy.

