

## Privacy notice concerning the Bioretec Group whistleblowing notification channel

Drafted on 11 February 2025

### 1 Controller and contact details for register matters

Bioretec is made up of different legal entities, the details of which can be found on the Bioretec website. This Privacy Notice is issued on behalf of the Bioretec Group so when we mention “we”, “us” or “our” in this Privacy Notice, we are referring to the relevant company in the Bioretec Group responsible for processing your data. If you have any queries about the processing of your personal data, you can contact:

**Bioretec Ltd** ("the Company" or "we")

Yrittäjänkulma 5

FI-33710 Tampere, Finland

+358 20 778 9500

privacy@bioretec.com

### 2 For what purposes and on what basis do we process your personal data?

The purpose of the processing of personal data is to implement the whistleblowing notification channel and to process the notifications received. The data will be used to monitor and investigate misconduct and, where necessary, to establish, exercise or defend legal claims.

Bioretec's whistleblowing notification channel allows Bioretec's employees and other representatives of stakeholders and partners to report suspected acts or omissions concerning illegal activities which are punishable by law or administrative sanctions or which may seriously undermine the achievement of the public interest objective of the legislation, and where the suspected infringement concerns a field of law within the meaning of the Finnish Act on the Protection of Persons Reporting Infringements of European Union and National Law 1171/2022 (the “Whistleblower Act”), including financial services, products and markets, prevention of money laundering and terrorist financing, product safety and compliance, environmental protection, public health, protection of privacy and personal data, security of network and information systems, competition law, customs law and tax law. The legal basis for the processing is compliance with a legal obligation of the controller (Art. 6(1)(c) GDPR, section 6.1(2) of the Data Protection Act).

Through the whistleblowing notification channel, an individual can also report conduct that violates the Company's Code of Conduct, such as suspected bribery, corruption and conflicts of interest, disclosure of confidential information, discrimination, and human rights violations. In this case, the basis for processing is

our legitimate interest in ensuring the legality and ethics of our activities (Article 6(1)(f) of the GDPR). To the extent that such notifications include information relating to special categories of personal data, the processing of such data is necessary for the establishment, exercise, or defence of legal claims pursuant to Article 9(2)(f) of the GDPR.

### **3 What kind of personal data do we process and where do we collect it from?**

In the context of the whistleblowing channel, we may process following types of personal data about the whistleblower and the subject of the notification, as well as other related persons, such as witnesses:

- Contents of the notification, such as the name and contact details of the subject of the notification, a description of the breach or misconduct, the time and place, and any other information that the whistleblower considers relevant (depending on the nature of the notification, the personal data processed may include personal data relating to special categories of personal data).
- Names and contact details of any witnesses or other persons involved.
- Information related to the submission, processing, and communication of the notification (including notification code and status).
- Any other information provided by the whistleblower.

In addition, we store information of the persons processing the notifications coming through the whistleblowing channel. This information includes the name, job title, email address, system login information and logs concerning the use of the system.

The primary source of the data is the whistleblower themselves. In addition, the data will consist of information recorded during the process of handling whistleblowing notifications, such as information received from relevant staff and IT systems and during the consultation of the person who may be the subject of the report. Other sources of information will be used within the limits set by law.

### **4 To whom do we disclose or transfer data?**

Notifications received through the whistleblowing channel are handled by the Company's whistleblowing team. In addition, a very limited number of other people may be involved in the processing of the notifications, such as legal advisors involved in the processing of notifications, experts authorised by the Company and internal audit staff.

In case, the identity of the whistleblower is known, it will not be disclosed to persons other than those responsible for receiving and following up on notifications without the express consent of the whistleblower. However, the identity of the whistleblower may be disclosed if the disclosure is necessary for the competent authority to establish the validity of the report, for the pre-trial investigation authorities or the public prosecutor to perform their duties, or for the establishment, exercise, or the defense of legal claims in accordance with the Whistleblower Act.

We use our trusted service providers to manage the notification channel system and process notifications. The technical implementation of the notification channel system is provided by the Finland Chamber of Commerce, which safeguards the anonymity of the person sending the notification by removing metadata, such as IP addresses, from the communication. Our service providers will process your personal data only to the extent necessary to implement the whistleblowing notification channel. We take care of your privacy by entering into data processing agreements with the service providers that process your personal data.

## **5 Do we transfer data outside the EU or EEA?**

Personal data is not transferred outside the EU or EEA.

## **6 How do we protect your data and how long do we store it?**

Access to the system is only granted to persons whose job entitles them to process the data and who are bound by confidentiality obligations. Each user has their own personal username and password for the system. The data are collected in databases protected by firewalls, passwords, and other technical means. Processors of personal data follow comprehensive information security procedures and have processes in place to detect and prevent security breaches.

The data in the register will be kept for as long as necessary to fulfil the purpose of the processing or pursuant to legal obligations. The data will be automatically removed five years after receipt of the notification unless a longer period is necessary for the exercise of rights or obligations laid down by law or for the establishment, exercise, or defense of legal claims.

## **7 Your rights as a data subject in relation to data processing**

As a data subject, you have the following rights under the GDPR and the Finnish Data Protection Act. However, these rights are not absolute - the exercise and/or restriction of these rights is governed by law and any government regulations and guidelines, which are not exhaustively described below. For example, the Company may have the right to restrict the exercise of the rights set out below where this is necessary and proportionate to safeguard the investigation and the follow-up of the notification or to protect the identity of the whistleblower. Requests concerning the rights of data subjects should be sent to the address provided in section 1.

- Right of access and right to request rectification and erasure of data
  - You have the right to inspect the data concerning yourself that are stored in the personal data file, and the right to request the rectification of inaccurate data and the deletion of data, if there are lawful grounds for such request.
- Right to object and restriction of processing
  - Where processing is based on legitimate interests, you have the right to object to the processing of your data on grounds relating to your particular situation, and the right to request restriction of the

processing of your data. When making such a request, you must identify the particular situation on basis of which you object to the processing. The controller may refuse to comply with the request only on grounds provided for by law.

- Where processing is based on our legal obligation, the right to object or restrict processing does not apply.
- Right to lodge a complaint with a supervisory authority
  - You have the right to lodge a complaint with a supervisory authority, in particular in the EU Member State of your habitual residence, place of work or place of the alleged infringement, if you believe that the processing of personal data concerning you infringes the EU General Data Protection Regulation.
- The information processed in the whistleblowing notification channel is never subject to automated decision-making.