

APPENDIX 2

Acceptable Use Policy

to the Bindex® License Agreement between Prevenova GmbH and the Licensee — Version September 2026

This Acceptable Use Policy (the "Policy") sets out the terms that apply to **Authorised Users** who access and use the Bindex® Software (the "Software") and the Bindex® Device (the "Device") provided under the Bindex® License Agreement (the "Agreement") between Prevenova GmbH, Baarerstrasse 19, 6300 Zug, Switzerland, acting as authorised sub-licensor (the "Sub-Licensor"), and the Licensee. Bone Index Finland Oy, Kuopio, Finland (the "IP Owner") is the manufacturer of the Device and the owner of all intellectual property rights in the Software and the Device. Capitalised terms not defined in this Policy have the meaning given to them in the Agreement. By using the Software, Authorised Users agree to comply with this Policy and act in accordance with the terms outlined below. The Licensee is responsible for ensuring that all of its Authorised Users are made aware of and comply with this Policy.

1. Obligations of Authorised Users

Each Authorised User must:

1.1 Follow Instructions: Read and comply with all user manuals, training materials, and guidance provided by the Sub-Licensor or the IP Owner.

1.2 Intended Use: Use the Software and the Device only for their intended purpose of facilitating osteoporosis screening and generating bone density assessments.

1.3 Lawful Use: Operate the Software and the Device in compliance with all applicable laws, regulations, and medical standards.

1.4 Good Faith: Use the Software and the Device in good faith, exercising care and diligence in their operation.

1.5 Training: Only use the Software and the Device after having completed the user training provided or approved by the Sub-Licensor.

2. Prohibited Activities

Authorised Users must not:

2.1 Unauthorised Modifications: Alter, modify, copy, or create derivative works of the Software.

2.2 Harmful Data: Upload, transmit, or input any data containing viruses, malware, or other harmful components.

2.3 Misrepresentation: Input false or fabricated patient data into the Software.

2.4 Sharing Credentials: Share login credentials or access to the Software with unauthorised individuals.

2.5 Reverse Engineering: Attempt to reverse-engineer, decompile, or disassemble the Software, or open, modify, or tamper with the Device.

2.6 Misuse: Use the Software or the Device in any way that is outside their intended scope or that could damage the reputation of the Sub-Licensor or the IP Owner, or the integrity of the Software or the Device.

3. Security and Data Integrity

3.1 System Security: Authorised Users must ensure that the systems and devices used to access the Software are secure and free from viruses or malware.

3.2 Data Accuracy: Input only accurate and truthful patient information as required by the Software.

3.3 Incident Reporting: Report any misuse, suspected security breaches, or malfunctions of the Software or the Device to the Licensee or the Sub-Licensors promptly.

4. Compliance Monitoring

4.1 The Sub-Licensors, and the IP Owner acting through the Sub-Licensors, reserve the right to monitor usage of the Software to ensure compliance with this Policy, in accordance with the data protection provisions of the Agreement.

5. Consequences of Non-Compliance

5.1 Non-compliance with this Policy may result in:

- a) Revocation of access to the Software for the Authorised User concerned;
- b) Suspension or termination of the Licensee's licence under the Agreement; and/or
- c) Legal action as deemed necessary by the Sub-Licensors and/or the IP Owner.

5.2 A breach of this Policy by an Authorised User is deemed a breach of the Agreement by the Licensee.

6. Amendments

6.1 The Sub-Licensors may amend this Policy from time to time to ensure the security and appropriate use of the Software and the Device, including where required by the IP Owner. Updated versions will be communicated to the Licensee in writing and apply from the date stated in the communication.