Document Owner	Group CFO
Document Holder	Group CFO
Approval	Board of directors of Bentley Endovascular Group AB (publ)
Date of Approval	2025-04-29

Data Privacy Policy

Bentley Endovascular Group AB (publ)

TABLE OF CONTENT

1. INTRODUCTION

Bentley Endovascular Group AB (publ) (hereinafter "Company"; Bentley Endovascular Group AB (publ) as well as its subsidiaries hereinafter "Bentley", the "Group" or "we") is an international medical technology company with headquarters in Sweden and global subsidiaries.

This Policy is Bentley's internal, binding Policy for the collection, processing, transfer and use of all personal data. It is designed to protect personal data of data subjects and to maintain an adequate level of protection by ensuring that all data protection-related activities comply with all applicable data protection regulations, including the European General Data Protection Regulation ("GDPR") and, for the Bentley's Swiss operations, Swiss FADP

2. PURPOSE

The board of directors (the "**Board**") of Bentley Endovascular Group AB (publ) has adopted this Data privacy Policy (the "**Policy**").

The purpose of the Policy is to ensure compliance with laws and regulations applicable to data collection, storage, use, transmission, disclosure to third parties and retention of Personal and sensitive personal data (also referred to as personal and sensitive personal information respectively in this Policy).

3. SCOPE

The Policy applies to all permanent and temporary employees of the Company (including any of its intermediaries, subsidiaries or associated companies). It also applies to any individual or corporate entity associated with the Company or who performs functions in relation to, or for and on behalf of, the Company, including, but not limited to, directors, agency workers, casual workers, contractors, consultants, and suppliers. All employees and associated persons are expected to adhere to the principles set out in this Policy.

4. PRINCIPLES

4.1 The Board is ultimately responsible for this Policy, but it resides with the Group CFO who is also the Document holder/owner. This Policy shall be reviewed at least annually for necessary updates. As Bentley's business and regulatory requirements are constantly changing, it is critical for the Group CFO to ensure that this Policy as well as instructions hereunder are updated regularly. The Group CFO is responsible for maintaining proper documentation of any changes to the Policy.

4.2 This Policy must be observed in all dealings with personal data of natural or legal persons, especially in the collection, processing and transfer of data. It does not apply to anonymized data, but applies personally to all employees, contractors and officers of Bentley. Adherence to this Policy is the responsibility of both Bentley and all individuals affected by it. It is

implemented by Bentley's management and is binding on all those whom it applies. It supplements, but does not replace, existing national data protection regulations. Statutory legal obligations remain unaffected by this Policy. In the event of any conflict or inconsistency between statutory provisions/law and obligations under this Policy, statutory law shall prevail. The provisions of this Policy are binding even in the absence of data protection statutory provision/law on. Supervisors are responsible for ensuring that all newly hired employees and consultants are informed about this Policy.

5. DATA PROTECTION OFFICER

The Group CFO shall appoint one or more data protection officers ("**DPO**") as required by the applicable law, for Bentley. The DPO shall have the full support of Bentley's management in the performance of his/her duties. The DPO is responsible for ensuring compliance with statutory data privacy regulations and the provisions of this Policy. The DPO is available to Bentley's management to advise on the fulfilment of Bentley's obligations under data protection law, to monitor compliance with legal requirements and any risks, and is responsible for consultation with the supervisory authorities. In all other respects, the DPO works conscientiously and in accordance with his or her expertise and is not bound by instructions. The DPO can be contacted confidentially at any time with complaints, requests for information and other data protection concerns. The DPO can be contacted as follows: Datenschutz_BI@bentley.global.

6. ROLES AND RESPONSIBILITIES

Roles	Responsibilities
Board	• Approves the Policy.
Group CEO	Strategic responsibility and escalation of items from the Group CFO.
Group CFO	• Overall responsibility for the Policy and the supporting instructions (Document Owner). • Responsible for conducting regular assessment to measure the status of implementation and support business areas to improve maturity based on the business needs and risk exposures. • Responsible for proposing updates to the Policy and documenting such changes (as Document Holder). • Approval of Group level guidelines and instructions under this Policy, if required.

	• Report to the Group CEO & Board.
IT Manager/Head of IT	• Overall responsibility for implementing technical and organisation measures necessary to meet the requirements of the GDPR. • Ensures that Bentley always have updated Article 30 registers of their processing of personal data. • Reports to Group CFO.
DPO	• Overall responsibility for compliance with and implementation of the requirements applicable to the processing of personal data. • Be the contact person both internally and externally for Data protection related inquiries and incidents. • Cooperate with the supervisory authority, in for example supervisory matters. • Handling reports and requests under this Policy. • Report general risk assessment, implementation updates and specific high-risk situations to Group CFO. • Provide appropriate data privacy information material to educate employees. • Report to the Group CFO.
Employees, contractors and external parties	• Every employee, contractor and external party has a responsibility to comply with this Policy.

7. PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA

The following legal principles must be observed when processing personal data:

7.1 Lawfulness, fairness and transparency: Personal data is collected in a lawful, fair and transparent manner in relation to the data subject. The data subject shall be informed about any data processing and be able to see the purpose of the data processing, which controller he or she can contact and whether or to which third parties the data will be transmitted.

7.2 Purpose limitation: The use of personal data must serve a previously defined, clear and legitimate purpose and may not be carried out in a manner incompatible with these

purposes. Subsequent changes of purpose are only permitted in exceptional cases and require justification.

7.3 Data minimization, storage limitation: Before processing personal data, it shall always be checked whether and to what extent the purpose of the processing is achieved with the intended approach. If the purpose can also be achieved without recourse to personal data, e.g. by anonymized or pseudonymized data, this milder approach shall be preferred. Subject to other governmental regulations, the retention of personal data for purposes that are unrelated or future is impermissible. Personal data shall only be stored for as long as it is necessary for the purpose of processing. As soon as the legal or operational retention periods have expired, personal data must be deleted.

7.4 Accuracy: The accuracy, completeness and up-to-datedness of the personal data collected shall be ensured. Otherwise, incorrect, incomplete and no longer current data shall be corrected, supplemented, updated or deleted without delay.

7.5 Integrity, confidentiality: Personal data shall be treated confidentially and appropriate technical as well as organizational measures shall be taken to ensure adequate protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

7.6 Accountability: In accordance with Article 30 of GDPR, the Company shall keep a register of all data processing activities, in particular to demonstrate compliance with the principles set out in this Policy.

8. LAWFULNESS OF DATA PROCESSING

According to applicable data protection legislation, processing of personal data is only lawful if at least one of the following legal grounds exists:

8.1 Consent to data processing: The data subject may give his or her consent to in particular processing of personal data for advertising purposes. A valid consent needs to be freely given, specific, informed and unambiguous. The data subject must be informed comprehensively before giving consent. The declaration of consent must be voluntary and generally provided in writing or electronically. The consent must be properly documented. The data subject also needs to be able to withdraw his or her consent at any time. If the consent to for example processing of personal data for advertising purposes is withdrawn, you cannot use the personal data in question for advertising purposes.

8.2 Data processing based on contractual relations: Processing is permitted insofar as it is necessary for the establishment, performance, termination or fulfilment of an existing contract, or the processing is necessary for the performance or implementation of pre-contractual measures or a legal obligation of the controller.

8.3 The processing is necessary in order to protect vital interests: Processing is permitted insofar as it is necessary to protect the vital interests of the data subject or another natural person.

8.4 Data Processing based on the legitimate interest of the controller: Processing is permitted insofar as it is necessary to fulfil a legitimate interest of the controller or a third party, unless

such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data. This shall be carefully checked before any processing.

8.5 Legal obligation to process personal data: Processing is permitted if it is necessary to fulfill a legal obligation. A common example is processing of personal data for accounting purposes.

8.6 Processing of special categories of personal data: Special categories of personal data (for example personal data concerning health, ethnic origin or religious beliefs) are in principle prohibited to process. Special categories of personal data may however be processed if for example the data subject's explicit consent has been obtained or if it is required for the assertion, exercise or defense of legal claims against the data subject.

8.7 If personal data is processed, collected or used on websites or in apps or by means of cookies, there is always an obligation to inform the data subject about this by means of notices in an easily recognizable, directly accessible and permanently available manner. A valid consent from the person in question (freely given, specific, informed and unambiguous) is required when using non-essential cookies such as statistic cookies or marketing cookies. The same applies to profiling, the creation of usage profiles to evaluate internet usage behaviour. Profiling is only permitted on the basis of legal permission, or the consent of the person concerned.

9. RETENTION PERIODS

A fundamental requirement of the GDPR is that personal data shall not be kept in a form which permits identification of individuals for longer than what is necessary for the purposes for which the personal data is processed. Each organization within Bentey and its employees are responsible for not processing any personal data longer than necessary and for complying with any additional procedures and documents adopted by Bentley regarding retention periods.

10. LAWFULNESS OF DATA TRANSFERS

A transfer of personal data to third parties is only permitted under the conditions of this Policy for lawful data processing. Consequently, a transfer is only lawful if it is permitted by law and it serves a predetermined purpose. If personal data is to be transferred to a third country outside the EU/EEA appropriate safeguards need to be put in place.

11. DATA PROCESSING ON BENTLEY'S BEHALF

11.1 If an external natural or legal person, authority, institution or other body processes personal data on behalf of Bentley as a processor, a data processing agreement with that external body shall be concluded in writing with the mandatory content set out in the applicable law (Article 28 of the GDPR). The data processing must be carried out in accordance with the specific instructions of the controller (i.e. the relevant Bentley entity).

11.2 The controller shall be responsible for the legally compliant execution and implementation of the processing. It shall carefully select the processor, especially according to the professional suitability, the quality of its technical-organizational data security standards or comparable indicators of reliability.

11.3 The controller shall ensure the highest possible level of data protection for the processor by issuing instructions, e.g. with regard to data security measures, responsibilities and accountabilities between the processor and the controller.

12. RIGHTS OF DATA SUBJECTS

Data subjects may exercise the following data protection rights, provided that the factual requirements of the respective rights are met:

12.1 Right to information: Every data subject has the right to request information as to whether personal data relating to him or her is being processed in the Company and, if so, which data is being stored, for what purpose, from what source and for how long. In the event of data being transferred to third parties, information must also be provided about the identity of the recipient and the categories of recipients.

Before providing the information or respond to any other request from the data subject, the controller shall establish the identity of the data subject and, if necessary, take measures to dispel any doubts that may arise as to the identity of the requesting person.

12.2 Right of access: Every data subject has the right to obtain confirmation as to whether personal data relating to him or her is being processed in the Company and, if so, information about how the Company processes the personal data and to receive a copy of the personal data.

12.3 Right to rectification: Every data subject may request the immediate correction or completion of personal data concerning him/her that is inaccurate or incomplete.

12.4 Right to erasure ("right to be forgotten"): Every data subject shall be entitled to the immediate erasure of personal data concerning him or her as soon as one of the following grounds for erasure is relevant:

- The purpose of the data processing does not exist or no longer exists.
- A legal basis for the data processing is missing or has ceased to exist in that the data subject has revoked his or her consent.
- The data subject objects to the data processing and there are no overriding legitimate grounds for the processing.
- The personal data is processed for direct marketing purposes and the data subject objects to the processing.
- The data processing is unlawful.

- The processing of personal data is not (or is no longer) necessary for compliance with a legal obligation or for the assertion, exercise or defense of legal claims.
- If personal data has been made public and there is an obligation to erase it, further responsible parties must be informed that the data subject has requested them to erase all links to the relevant personal data or copies or duplicates thereof.

12.5 Right to restriction of processing: The data subject shall have the right to restrict the processing of personal data concerning him or her as soon as one of the following grounds is relevant:

- The data subject disputes the accuracy of the personal data. A restriction is made for the period in which the person responsible verifies the accuracy
- The data processing is unlawful, but the data subject requests the restriction of use instead of deletion of the personal data.
- The personal data is no longer required by the controller for the purposes of processing, but the data subject needs it for the assertion, exercise or defence of legal claims.
- The data subject has objected to the processing. Restriction takes place for the period during which the controller reviews the objection.

After an effective restriction of processing, the personal data concerned may be processed only with the consent of the data subject or for the establishment, exercise or defense of legal claims or for the protection of the rights of others or on the basis of an important public interest. The person concerned shall be informed about the lifting of the restriction.

12.6 Right to data portability: If data processing is based on consent or is necessary for the performance of a contract, the data subject has the right to transfer the personal data that he or she has provided to the Company to another controller in a structured, commonly used and machine-readable format, insofar as this is technically possible.

12.7 Right to object: Every data subject has the right to object at any time to data processing that is based on consent or is necessary to protect legitimate interests. For this, the result of an assessment must show that the interest of the data subject worthy of protection resulting from a special situation outweighs the interest of the Company in the processing. There is no right to object if the processing serves the assertion, exercise or defence of legal claims.

12.8 Right to lodge a complaint: In addition, every data subject has the right to lodge a complaint with the competent supervisory authority if he or she believes that the processing of his or her personal data has been carried out unlawfully.

To exercise a data protection right, the data subject may contact the DPO. The data subject's request shall be assessed and handled promptly, but no later than one month after the Company received the request. Each employee is therefore responsible for reporting any data subject request that they become aware of to their supervisor and to the DPO. The DPO is thereafter responsible for investigating and handling the request, with assistance from other employees.

13. DATA PROTECTION CONTROL

13.1 To ensure an adequate level of protection and compliance with applicable data protection regulations, compliance with this Policy must be regularly monitored through audits and other control mechanisms by DPO.

13.2 The results of each audit shall be documented and reported to the IT Manager/Head of IT & Group CFO. A data protection audit is successfully completed when all documented deficiencies have been remedied by implementing appropriate measures. This shall be verified accordingly.

14. CONFIDENTIALITY OF DATA PROCESSING

14.1 All employees are obliged to comply with data protection (data secrecy). Employees are prohibited from unauthorized collection, processing or use of personal data. If an employee acts without authorization, for example if he or she processes personal data without being instructed or authorized to do so in the performance of his or her duties, they might face a disciplinary action.

14.2 All employees must sign a confidentiality agreement before starting work. they must ensure that the personal data obtained in the course of their work will not be used for private or economic interests, disclosed to unauthorized persons or made accessible in any other way. This obligation shall survive the termination of the employment relationship. Upon commencement of employment, the employee shall be informed of his or her obligation to maintain confidentiality and shall be required to do so in writing. To ensure a high level of confidentiality, employees may only be granted access to personal data to the extent that is specifically required for the performance of their duties (need-to-know principle). A detailed and complete authorization concept/Policy/instructions shall be established and carefully maintained, providing employees with defined access authorizations/rights in accordance with their roles and responsibilities.

15. PERSONAL DATA BREACHES

15.1 A "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Common examples of Personal Data Breaches are that a server is hacked or that a computer containing personal data is stolen.

15.2 Both controllers and processors have obligations under the GDPR in the event of a Personal Data Breach. In essence, the controller is responsible for notifying the competent supervisory authority of a Personal Data Breach no later than 72 hours after becoming aware of it and informing the data subjects affected by the Personal Data Breach without undue delay. The processor shall inform the controller without undue delay after becoming aware of a Personal Data Breach.

15.3 In the event of a Personal Data Breach, a violation of this Policy or other personal data regulations, the employee responsible shall immediately report the data breach to his or her

supervisor and to the DPO. The report must include all information necessary to establish the facts, particularly the recipient, the specific personal data involved, and the nature and scope of the data affected by the incident. Each employee is responsible for reporting any Personal Data Breach that they become aware of to their supervisor/manager and to the DPO. The DPO is then responsible for investigating and dealing with the breach, with assistance of other employees.

15.4 If there is a reporting obligation to the supervisory authorities for the respective data breach, the DPO shall fulfil this obligation without delay. If a data breach, a violation of this Policy or a violation of other data protection regulations has been caused negligently or intentionally, there may be consequences under employment law. In addition, criminal and civil sanctions may be considered, such as the assertion of claims for damages.

16. DATA PROTECTION IMPACT ASSESSMENT

If a form of processing of personal data is likely to present a high risk to the rights and freedoms of data subjects, each data-processing department shall be required to conduct a data protection impact assessment of the intended data processing in advance. The DPO is responsible for performing Data Protection Impact Assessments, with assistance from other employees.

17. INVESTIGATIONS

17.1 All internal company investigations must comply with the applicable standards on data protection and data protection obligations. Data processing in connection with the investigation must be proportionate to the objective of the investigation and to the interests of the data subjects to be protected, i.e. suitable, necessary and appropriate. Internal company investigations include measures aimed at preventing, investigating or establishing a serious breach of duty under employment law or a criminal offense.

17.2 Ensure that the data protection officer is involved and consulted on the form, scope and other details of all investigative measures.

17.3 The person concerned shall be informed without delay of the fact that he/she is the subject of an investigation and of the measures taken.

18. ASSOCIATED DOCUMENTS

- Information Security Policy
- IT Policy
- Business Continuity Policy

* * * *