Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR no. 33 96 35 56
Weidekampsgade 6
2300 Copenhagen S

Phone: 36102030
www.deloitte.dk

NOVICELL ApS

Independent auditor's ISAE 3000 Type 2 Assurance Report on information security and measures pursuant to data processing agreements with data controllers for the period from 1 June 2024 to 31 May 2025

November 2025

Table of contents

Section 1: Independent auditor's report

To: Novicell ApS, their Clients and their Auditors

Scope

We were engaged to provide assurance on Novicell ApS's description in Section 3, in accordance with the data processing agreement with data controllers, for the period from 1 June 2024 to 31 May 2025, and on the design and operating effectiveness of controls related to the control objectives set out in that description.

Novicell ApS uses the following sub-processors:

- Microsoft (Azure Open AI Service and Microsoft Office 365)
  Novicell uses Microsoft Azure for its own solutions as well as for those of its customers. For Novicell, Microsoft provides both a hosting platform and licences for services such as Microsoft 365, Intune, Defender, SharePoint, and others. Physical security of Microsoft data centres is the responsibility of Microsoft, while Novicell is responsible for the use of the services provided. For customers, only Microsoft Azure is utilised, which includes databases, app services, servers, and microservices.

- Amazon Web Services (AWS)
  Novicell uses AWS for both its own and its customers' solutions. Amazon provides the hosting platform. Physical security of Amazon's data centres is Amazon's responsibility, while Novicell is responsible for the use of the web services provided by Amazon. For customers, only AWS is utilised, which includes databases, app services, servers, and microservices.

- Dynamicweb Software A/S
  Novicell uses the Dynamicweb platform to host customers and employs DW as a CMS. Novicell acts solely as a reseller of the licences for Dynamicweb. DW is responsible for all infrastructure, backup, and security.

- Umbraco A/S
  Umbraco Cloud is a SaaS solution for hosting the Umbraco CMS, primarily hosted on Microsoft Azure's infrastructure. Umbraco Cloud is responsible for the infrastructure, backup, security, and automatic deployment of minor releases.

- Platform.sh SAS
  Platform.sh is a SaaS solution comparable to Umbraco Cloud but primarily utilises AWS as its infrastructure platform. Platform.sh has recently changed its name to Upsun. Upsun provides relevant services for customers' solutions and is responsible for infrastructure, backup, and security.

- WP Engine Inc.
  WP Engine is a managed WordPress hosting provider that delivers web servers, security, updates, and performance optimisations specifically tailored for WordPress. It serves as a platform for WordPress websites and provides tools and environments for developers, agencies, and businesses to build, deploy, and scale WordPress sites. WP Engine is responsible for hosting and infrastructure, security, performance, backup, various developer tools, and customer support.

- Curanet A/S
  Curanet is Novicell's Virtual Data Center provider. They supply a VMware platform on which Novicell can deploy virtual machines. Curanet is responsible for all physical hardware, including equipment, cooling, and network infrastructure such as firewalls available to Novicell. Novicell manages network segregation, backup, and scaling of customers' solutions.

Novicell ApS's system description, as set out in Section 3, does not include control objectives or associated controls for the sub-processors.

Some of the control objectives listed in Novicell ApS's description of the Novicell ApS system can only be achieved if the complementary controls at the user organisations are suitably designed and operating effectively together with

the controls at Novicell ApS. The opinion does not include the suitability of the design, implementation and operating effectiveness of these complementary controls.

The information in Section 5, "Additional information provided by Novicell ApS" is presented by management of Novicell ApS to provide additional information and is not a part of Novicell's description of its system made available to user entities. The information has not been subjected to the procedures applied in the examination of the description of the system and of the suitability of the design and operating effectiveness of controls and, accordingly, we express no opinion on it

Novicell ApS's responsibilities

Novicell ApS is responsible for preparing the description and the accompanying assertion in Section 2, including the completeness, accuracy and the method of presentation of the description and assertion; providing the services covered by the description; stating the control objectives; and designing, and implementing controls to achieve the stated control objectives.

Service auditor's responsibilities

Our responsibility is to express an opinion on Novicell ApS's description regarding the design and operating effectiveness of controls related to the control objectives set out in that description, based on the procedures we have performed.

We conducted our engagement in accordance with International Standard on Assurance Engagements 3000, "Assurance Engagements Other than Audits or Reviews of Historical Financial Information", and additional requirements under Danish audit regulation to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are appropriately designed and operating effectively.

An assurance engagement to report on the description, design, and operating effectiveness of controls at Novicell ApS involves performing procedures to obtain evidence regarding the disclosures in Novicell ApS's system description, as well as the design and operating effectiveness of controls. The procedures selected depend on the auditor's judgement, including the assessment of risks that the description may not be fairly presented, and that controls may not be appropriately designed or operating effectively. Our procedures included testing the operating effectiveness of those controls we considered necessary to provide reasonable assurance that the control objectives set out in the description were achieved.

An assurance engagement of this type also includes evaluating the overall presentation of the description, the appropriateness of the objectives set out therein, and the suitability of the criteria specified by Novicell ApS and described in Section 2.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Service auditor's independence and quality control

We have complied with the requirements for independence and other ethical obligations set out in the IESBA Code of Ethics, which is based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behaviour.

Deloitte Statsautoriseret Revisionspartnerselskab applies the International Standard on Quality Management 1 (ISQM 1), which requires the firm to design, implement, and operate a system of quality management, including policies and procedures addressing compliance with ethical requirements, professional standards, and applicable legal and regulatory obligations.

Limitations of controls at a data processor

Novicell ApS's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Novicell ApS's services that an individual data controller may consider important in their particular circumstances. Additionally, due to their nature, controls at a data processor may not prevent or detect personal data breaches.

Basis for qualified opinion

We have noted that some controls related to "Control objective B: Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing" and "Control objective C: Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing" have not worked effectively throughout the audit period. Based on this we qualify our opinion on the achievement of these control objectives. Refer to Section 4 for further details.

Qualified opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in Management's assertion in Section 2. In our opinion, except for the matters described in the Basis for qualified opinion paragraph:

a) The description fairly presents Novicell ApS's services as designed and implemented throughout the period from 1 June 2024 to 31 May 2025; and

b) The controls related to the control objectives stated in the description were appropriately designed throughout the period from 1 June 2024 to 31 May 2025; and

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 June 2024 to 31 May 2025.

Description of tests of controls

The specific controls tested, and the nature, timing and results of those tests are listed in Section 4.

Intended users and purpose

This report, together with the description of tests of controls in Section 4, is intended solely for data controllers who have used Novicell ApS's services and who have sufficient understanding to consider it alongside other information, including information on checks carried out by the data controllers themselves, when assessing compliance with the requirements of the GDPR.

Copenhagen, 24 November 2025

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR no. 33 96 35 56

Thomas Kühn
Partner, state-authorised public accountant

Michael Bagger
Partner

Section 2: Management's assertion

The accompanying description has been prepared for use by Novicell ApS's customers who have utilised Novicell ApS's services and who have sufficient understanding to assess the description alongside other information, including details of checks carried out by the data controllers themselves, when evaluating compliance with the requirements of the EU Regulation on the protection of natural persons, the General Data Protection Regulation.
Novicell ApS confirms that:

1) The accompanying description in Section 3 fairly presents the controls relevant to Novicell ApS's services, which have processed personal data for data controllers subject to the GDPR, throughout the period from 1 June 2024 to 31 May 2025. The criteria used in making this assertion were that the accompanying description:

    a) Presents how controls for Novicell ApS's services were designed and implemented, including:

        i) The types of services provided, including the types of personal data processed;
        ii) The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete and restrict processing of personal data;
        iii) The procedures used to ensure that data processing has taken place in accordance with contract, instructions or agreement with the data controller;
        iv) The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality;
        v) The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation;
        vi) the data controller's ability to report the breach to the supervisory authority and inform the data subjects;
        vii) The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data, taking into account the risks presented by such processing, including accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data that is transmitted, stored, or otherwise processed;
        viii) Controls that we, in reference to the scope of the Novicell applications, have assumed would be implemented by the data controllers and which, if necessary to achieve the control objectives stated in the description, are identified in the description;
        ix) Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data.

    b) Contains relevant information about changes to Novicell ApS's services for processing personal data in the period from 1 June 2024 to 31 May 2025.

    c) Does not omit or distort information relevant to the scope of Novicell ApS's services described for the processing of personal data, while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Novicell ApS's services that individual data controllers might consider important in their particular circumstances.

2) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 June 2024 to 31 May 2025. The criteria used in making this statement were that:

    a) The risks that threatened achievement of the control objectives stated in the description were identified;

    b) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved, with the exception of control objective B and control objective C, where inadequate controls have been noted to such a degree that the control objectives cannot be fulfilled.

c) The controls were consistently applied as designed throughout the period from 1 June 2024 to 31 May 2025, including that manual controls were performed by persons with the appropriate competence and authority.

Appropriate technical and organisational safeguards were established and maintained to comply with the agreements with data controllers, sound data processing practices, and the relevant requirements for data processors in accordance with the Regulation.

Aarhus, 24 November 2025

Novicell ApS

Kristian Rasmussen
CFO

Section 3: Management's description of Novicell's services

Introduction

This system description relates to the personal data protection controls for consultancy services and hosting activities at Novicell ApS including Novicell Design ApS, named Novicell in this description.

As a consultancy agency and hosting provider, Novicell is responsible for implementing control systems that protect personal data in order to fulfil legal responsibilities, contractual obligations, and good practice. Only the 'Consultancy services' and 'Hosting activities' described below are within the scope of this ISAE 3000 report.

This description is limited to the general standards for our services as described in Novicell's standard contract. Specific conditions – related to individual customer contracts – are not included.

Description of services

Novicell's services are tailored to the specific customer, and the specific customer terms are described in individual contracts. For each service area, a standard contract is used as the foundation, and individual adjustments and addendums can be included. Processing activities of personal data are agreed upon in a data protection agreement that includes any customer-specific requirements. Customers can buy services from one or more areas. The following service areas are a subset of the overall services offered by Novicell and represent those within the scope of this assurance report:

Hosting: Customers hosted on dedicated hardware, dedicated virtualised servers or shared servers. Novicell is responsible for networking, backup and system software. Physical security responsibility is assigned to a housing partner.

Consultancy: Customers who hire Novicell consultants (development, design, strategy, enterprise architecture) to work under customer direction. Novicell is responsible for the consultant's general personal data protection training and workstation security.

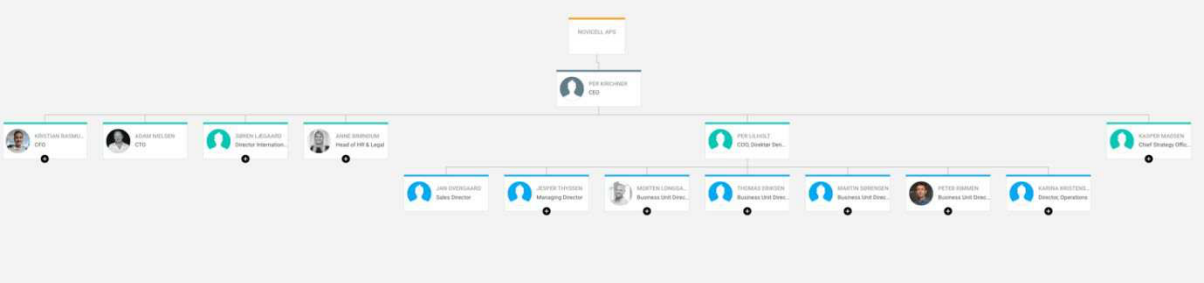
General control environment

The CEO is primarily responsible for personal data protection and the Information Security Policy at Novicell. Novicell's Information Security Policy forms the basis for data protection principles and guidelines. The Information Security Group is responsible for defining these principles and guidelines and for revising the Information Security Policy. The CFO is responsible for developing and implementing the relevant controls to ensure compliance with the Information Security Policy. The Information Security Group reports directly to the CEO. The Information Security Group currently consists of:

a. Per Lilholt, COO
b. Adam Nielsen, CTO
c. Martin Sørensen, Business Unit Director, Commerce
d. Ulrich Lander Madsen, Head of Cloud Services
e. Anne Brøndum, Head of HR & Legal
f. Kristian Rasmusssen, CFO

Members of the Information Security Group are required to keep up to date with developments in information security and to attend relevant training, as necessary. The Information Security Group reviews the Information Security Policy, as well as the associated principles and guidelines, annually to ensure the policy complies with current legislation and contractual obligations. Concurrently, the risk assessment is evaluated. Information security or personal data incidents are reported to the Information Security Group.

Organisational chart



Information Security Policy and organisational principles

To ensure coherence with the Information Security Policy and the organisation, the Information Security Group maintains the InfoSec Employee Manual that clearly communicates the Information Security Policy's principles and guidelines in everyday practical terms. Where applicable, the InfoSec Employee Manual is divided into areas specific for the service areas. The employee's department manager is responsible for communicating guidelines that ensure compliance with the Information Security Policy. Updates to the Information Security Policy and the InfoSec Employee Manual are announced to employees. The Information Security Group has delegated the day-to-day operations to the Legal Team. The Legal Team is the single point of contact for both employees and customers regarding data protection and handling of personal data.

Employee safety

At Novicell, HR activities related to information security are managed by the Finance, HR, and Legal departments, as well as by each employee's manager. Responsibility for information security is defined within each employee's job description and terms of employment. Employees receive training, guidelines, and information regarding information security through their department manager, who ensures that the level of training is appropriate to the employees' duties, responsibilities, and skills. This includes information about immediate threats and relevant resources for queries concerning information security. Each employee signs a confidentiality clause as part of their employment contract. Additionally, each manager annually confirms the implementation of the InfoSec Employee Guide within their respective team. Employees are responsible for complying with the Information Security Policy relevant to their individual duties and for reporting personal data incidents to the Legal team.

Risk assessment

For the various Novicell service areas, an annual risk assessment is carried out. The risk assessment describes the identified risks and the controls in place to mitigate them. The CFO is primarily responsible for the risk assessment, and the Information Security Group is responsible for conducting the assessment annually.

The risks associated with the various Novicell service areas vary, as responsibility for different parts of the complete security lifecycle is shared among Novicell, its customers, and its providers. The categories of personal data also differ with each customer; consequently, all personal data is treated as sensitive personal data. The InfoSec Employee Guide reflects this categorisation and the variability across service areas.

Control objectives and controls

Control objective A: *Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistently with the data processing agreement entered into.*

A set of procedures are implemented to govern the overall processing of personal information.

Control objective B: *Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.*

Physical access
Locations that contain production systems with personal data are only accessible to authorised personal with professional duties, and access is only granted with key card and code. The physical access control for production systems is the responsibility of the housing provider and the private cloud provider.

Logical access
At all office, home, and remote working locations, personal data is protected by workstation disk encryption and strong, unique passwords. Password requirements are enforced on all Novicell user accounts.

Systems storing or providing access to personal data are configured so that only employees for whom access is relevant have permission. All user accounts are individual; where this is not possible due to system constraints, multifactor authentication has been enabled where feasible.

Acquisition and maintenance of infrastructure
Company networks and devices are designed, deployed, and operated to provide appropriate levels of protection for the data being accessed and transmitted.

The Cloud Services department is responsible for the company's network design and operation. Ongoing maintenance is documented in Novicell's case management system, and significant changes to network design and configurations are recorded by Cloud Services.

Network documentation and patching status are reviewed at least annually.

System software
System software is updated according to Novicell's procedures and vendors' guidelines. Each quarter, servers are reviewed for OS version and latest date of OS update and patch.

The Cloud Services department is responsible for maintaining system software and the control hereof.

Control objective C: *Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.*

Processes and training are in place to continuously raise employee awareness of identifying personal data breaches. Monitoring of network traffic and logs of access to personal data are also established.

Control objective D: *Procedures and controls are complied with to ensure that personal data can be deleted or returned if arrangements are made with the data controller to this effect.*

Customer requests concerning their data subjects' right to erasure, right of access and right of data portability are logged and monitored by the Information Security Group.

Customer requests concerning their data subjects and controls as per the risk assessment are reported annually by the Finance, HR, and Legal departments. The report is presented to the Information Security Group.

Control objective E: *Procedures and controls are complied with to ensure that the data processor will only store personal data in accordance with the agreement with the data controller.*

Procedures are in place to ensure that data processing and storage take place only in the localities, countries, or regions approved by the data controller.

Control objective F: *Procedures and controls are complied with to ensure that only approved sub-processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.*

Established procedures ensure that Novicell uses only approved sub-processors as agreed, and that these sub-processors are subject to the same data protection obligations, technical and organisational measures to protect the rights of data subjects and the processing of personal data.

The list of approved and used sub-processors is continuously evaluated and updated with records and relevant information about each company. An annual risk assessment is conducted for each sub-processor to re-evaluate the associated risks. Reviews, certifications, and independent auditor's reports are collected to monitor each sub-processor's adequacy in securing the processing of personal data.

For further details on the controls, please refer to section 4.

Complementary controls of data controllers

As part of the delivery of services, the data controller must implement certain controls that are essential to achieving the control objectives specified in the description. These include:

- Considering the consequences related to the protection of personal data when change requests are raised
- Considering and testing new versions of systems at the implementation stage
- Managing the set-up and administration of their own users of the solution in the production environment
- Managing the set-up and administration of users from Novicell ApS who provide assistance in the customer's environment
- Ensuring that personal data are not included in support cases
- Considering how to ensure that personal data are anonymised when copied from production environments to test environments (typically necessary to enable a representative test of newly developed functionality before going live)
- Considering the need for penetration tests to be carried out by a recognised security company to verify the security of the developed solution
- Informing Novicell ApS about changes in employees who have access to sites shared between the customer and Novicell ApS
- Ensuring that any necessary DPIA is conducted and, based on this assessment, providing Novicell ApS with instructions for handling personal data
- Warranting that the purpose of processing personal data is lawful and fair, and that Novicell ApS is only provided with the personal data necessary to fulfil that purpose
- Being responsible for ensuring that a legal basis for processing exists at the time of transfer of personal data to Novicell ApS – including that any consent is freely given, specific, informed, unambiguous, and explicit, if required
- Warranting that the individuals to whom the personal data relate (the data subjects) have been sufficiently informed about the processing of their personal data
- Having primary responsibility for providing Novicell ApS with instructions regarding data processing and handling requests from data subjects concerning their rights
- Reporting any personal data breaches to the Danish Data Protection Agency.

Section 4: Management's description of Novicell ApS's control objectives and related controls, and independent service auditor's description of tests of controls and results

Introduction

This report is intended to provide the data controllers with information about the controls at Novicell ApS that may affect the processing of personal data, and to provide the data controllers with information about the design and implementation of the controls that were assessed.

This report, when combined with an understanding and assessment of the controls at the data controllers, is intended to assist the data controllers in assessing the risks related to the processing of personal data that may be affected by the controls at Novicell ApS.

Our assessment of Novicell ApS's controls was limited to the control objectives and related controls listed in the matrices in this section of the report and did not include all controls described in the system description, nor controls that may be in place at the data controllers. It is the responsibility of the data controllers to evaluate this information in relation to the controls in place at each data controller. If certain complementary controls are not in place at the data controller, Novicell ApS's controls may not compensate for such weaknesses.

The tests of controls performed consist of one or more of the following methods:

Test	Description
Corroborative inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed the performance of the control during the report period to evidence application of the specific control activity.
Examination of documentation/inspection	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Reperformance of monitoring activities or manual controls	Obtained documents used in the monitoring activity or manual control activity and independently reperformed the procedures. Compared any discrepancies identified with those identified by the responsible control owner.

Test of design and implementation

Our test of the design and operating effectiveness of controls includes such tests as we consider necessary to assess whether those controls performed, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the specific control objectives were achieved throughout the period from 1 June 2024 to 31 May 2025.

Management of Novicell ApS's description of its control objectives and related controls, and independent service auditor's description of tests of controls and results

Control objective A: Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistently with the data processing agreement entered into.

No.	Novicell's control activity	Deloitte's test	Result of test
A.1	Written procedures are in place which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis - and at least once a year - to determine whether the procedures need updating.	Checked by way of inspection that formalised procedures exist to ensure that personal data are processed only in accordance with instructions. Checked by way of inspection that the procedures include a requirement to assess at least once a year the need for updates, including in the event of changes to the data controller's instructions or to the data processing. Checked by way of inspection that procedures are up to date.	We have noted that the security committee's annual review of written procedures was conducted outside the assurance period. No further exceptions noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	Checked by way of inspection that management ensures that personal data are processed only in accordance with instructions. Checked by way of inspection, on a sample basis, documentation demonstrating that personal data processing operations are conducted consistently with instructions.	No exceptions noted.

No.	Novicell's control activity	Deloitte's test	Result of test
A.3	The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions.	Checked by way of inspection that formalised procedures exist ensuring verification that personal data are not processed in violation of the Regulation or other applicable legislation. Checked by way of inspection that procedures are in place to inform the data controller of cases where the processing of personal data is assessed to be in breach of legislation. Checked by way of inspection that the data controller was informed in cases where the processing of personal data was assessed to be in breach of legislation.	No exceptions noted.

Control objective B: Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	Novicell's control activity	Deloitte's test	Result of test
B.1	Written procedures exist that include a requirement for safeguards to be established for the processing of personal data in accordance with the agreement with the data controller. Assessments are made on a regular basis - and at least once a year - to determine whether the procedures should be updated.	Checked by way of inspection that formalised procedures exist to ensure establishment of the safeguards agreed. Checked by way of inspection that procedures are up to date. Checked by way of inspection of samples of data processing agreements that the agreed safeguards have been established.	We have noted that the security committee's annual review of written procedures was conducted outside the assurance period. No further exceptions noted.
B.2	The data processor has performed a risk assessment and, based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the safeguards agreed with the data controller.	Checked by way of inspection that formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security. Checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data. Checked by way of inspection that the data processor has implemented the technical measures ensuring an appropriate level of security consistent with the risk assessment. Checked by way of inspection that the data processor has implemented the safeguards agreed with the data controller.	No exceptions noted.
B.3	For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.	Checked by way of inspection, on a sample basis, documentation confirming that antivirus software has been installed on the systems and databases used in the processing of personal data.	No exceptions noted.

No.	Novicell's control activity	Deloitte's test	Result of test
		Checked by way of inspection that antivirus software is up to date.	
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	Checked by way of inspection that external access to systems and databases used in the processing of personal data takes place only through a secured firewall. Checked by way of inspection that the firewall has been configured in accordance with the relevant internal policy.	No exceptions noted.
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	Inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. Inspected network diagrams and other network documentation to ensure appropriate segmentation.	No exceptions noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	Checked by way of inspection that formalised procedures are in place for restricting users' access to personal data. Checked by way of inspection that formalised procedures are in place to ensure that users' access to personal data is consistent with their work-related needs. Deloitte has performed a walkthrough to verify that access to personal data is restricted to users with a work-related need. Checked by way of inspection that the technical measures support maintaining restrictions on users' work-related access to personal data.	We have noted that there are no formalised procedures in place for restricting users' access to personal data. We have noted a lack of management of user lists, which compromises the ability to ensure that access to personal data is appropriately restricted. We have noted, on a sample basis, a lack of functional segregation of duties in one system. We have noted, on a sample basis, that user access review is not effectively conducted.

No.	Novicell's control activity	Deloitte's test	Result of test
		Checked by way of inspection of samples of users' access to systems and databases that such access is restricted to the employees' work-related need. Checked by way of inspection that documentation exists that user access granted is evaluated and authorised on a regular basis —and at least once a year.	We noted that user access review is not conducted in a timely manner. No further exceptions noted.
B.7	System monitoring with an alarm feature has been established for the systems and databases used in the processing of personal data. This monitoring comprises: • Network monitoring • User access.	Checked by way of inspection that system monitoring with an alarm feature has been established for systems and databases used in the processing of personal data. Checked by way of inspection that alarms were appropriately followed up.	No exceptions noted.
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	Checked by way of inspection that formalised procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognised algorithm. Checked by way of inspection that technological encryption solutions have been available and active throughout the assurance period. Checked by way of inspection that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email. Inquired whether any unencrypted transmission of sensitive and confidential personal data has taken place during the assurance period and whether the data controllers have been appropriately informed thereof.	No exceptions noted.

No.	Novicell's control activity	Deloitte's test	Result of test

B.9	Logging of the following matters has been established in systems, databases and networks:
	
	• Activities performed by system administrators and others holding special rights
	• Security incidents comprising:
	  ○ Changes in log setups, including disabling of logging
	  ○ Changes in users' system rights
	  ○ Failed attempts to log on to systems, databases or networks.
	
	Logon data are protected against manipulation and technical errors, and are reviewed regularly.
		Checked by way of inspection that formalised procedures are in place for setting up logging of user activities in systems, databases or networks that are used to process and transmit personal data, including review of and follow-up on logs.
		
		Checked by way of inspection that logging of user activities in systems, databases or networks that are used to process or transmit personal data has been configured and activated.
		
		Checked by way of inspection that user activity data collected in logs are protected against manipulation or deletion.
		
		Checked by way of inspection of a sample of logging that the content of log files is as expected compared to the setup and that documentation confirms the follow-up performed and the response to any security incidents.
		
		Checked by way of inspection of a sample of logs that documentation confirms the follow-up performed on activities carried out by system administrators and others holding special rights.
			We have noted that there are no written procedures for setting up logging of user activities in systems, databases, or networks that are used to process and transmit personal data.
			
			No further exceptions noted.

B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.	Checked by way of walkthrough that personal data are used for development testing or similar for Novicell's customers, ensuring that the use is only in pseudonymised or anonymised form.	We have not been able to test the effectiveness of the control due to an insufficient and incomplete overview of personal data used for development, testing, or similar activities. No further exceptions noted.

No.	Novicell's control activity	Deloitte's test	Result of test
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	Checked by way of inspection that formalised procedures exist for regularly testing technical measures, including for performing vulnerability scans and penetration tests.	We have noted that there is no established procedure to regularly test technical measures through vulnerability scans or penetration tests. Furthermore, vulnerability scans and penetration tests have not been conducted during the assurance period. No further exceptions noted.
B.12	Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches.	Checked by way of inspection that formalised procedures exist for handling changes to systems, databases or networks, including handling of relevant updates, patches and security patches. Checked by way of inspection of extracts from technical security parameters and setups that systems, databases, or networks have been updated using agreed changes and relevant updates, patches and security patches.	No exceptions noted.
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	Checked by way of inspection that formalised procedures exist for granting and removing users' access to systems and databases used to process personal data. Deloitte has performed a walkthrough of the processes for granting and removing users' access and, based on inquiry, noted a lack of comprehensive management of user lists. Deloitte has performed a walkthrough to verify that employees' access to systems and databases has been authorised and is based on a work-related need.	We have noted that a formalised procedure is not in place for granting and removing users' access to systems and databases used to process personal data. We have noted that there is a lack of management of user lists, which compromises the ability to ensure that access to personal data is appropriately restricted. We have not been able to test the implementation and operating effectiveness of the user provisioning and deprovisioning controls, as

No.	Novicell's control activity	Deloitte's test	Result of test
		Deloitte has performed a walkthrough to verify that access to systems and databases for resigned or dismissed employees was deactivated or removed in a timely manner. Checked by way of inspection that documentation exists showing that granted user access is evaluated and authorised on a regular basis—and at least once a year.	we were unable to obtain a complete list of user creations and deletions for the systems. On a sample basis, we have noted a lack of functional segregation of duties in one system. On a sample basis, we have noted that user access reviews are not conducted effectively. We noted that user access review is not conducted in a timely manner. No further exceptions noted.
B.14	Systems and databases processing personal data that involve a high risk to data subjects are accessed, at a minimum, using two-factor authentication.	Checked by way of inspection that formalised procedures exist to ensure that two-factor authentication is applied in the processing of personal data that involves a high risk to the data subjects. Checked by way of inspection that users' access to processing personal data that involve a high risk to the data subjects may only take place by using two-factor authentication.	No exceptions noted.
B.15	Physical access safeguards have been established so as to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed.	Checked by way of inspection that formalised procedures exist to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed. Checked by way of inspection of documentation that, throughout the assurance period, only authorised persons have had physical access to premises	On a sample basis, we have noted that monitoring and review of a third-party service provider's assurance report, specifically regarding physical security measures, has not been performed. No further exceptions noted.

No.	Novicell's control activity	Deloitte's test	Result of test
		and data centres at which personal data are stored and processed. Checked by way of inspection that Novicell has a procedure for obtaining assurance reports from its sub-processors. Checked by way of inspection that Novicell has obtained the latest available assurance reports.	

Control objective C: Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

No.	Novicell's control activity	Deloitte's test	Result of test
C.1	Management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The IT security policy is based on the risk assessment performed. Assessments are made on a regular basis - and at least once a year - to determine whether the IT security policy should be updated.	Checked by way of inspection that an information security policy exists which Management has considered and approved within the past year. Checked by way of inspection of documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	We have noted that the security committee's annual review of written procedures was conducted outside the assurance period. No further exceptions noted.
C.2	Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.	Inspected documentation of Management's assessment that the information security policy generally meets the requirements for safeguards and the security of processing as set out in the data processing agreements entered into.	No exceptions noted.
C.3	The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant: • References from former employers • Diplomas.	Checked by way of inspection that formalised procedures are in place to ensure screening of the data processor's employees as part of the employment process. Deloitte has performed a walkthrough of the screening process as part of the employment process and, based on inquiry, noted whether references from former employers and diplomas have been verified and documented. Checked by way of inspection, on a sample basis, whether screening has been performed in accordance with procedure.	We have noted that references from former employers or diplomas are not obtained consistently. No further exceptions noted.

No.	Novicell's control activity	Deloitte's test	Result of test
C.4	Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.	Checked by way of inspection that samples of new hires employed during the assurance period that the relevant employees have signed a confidential agreement through the employment contract. Checked by way of inspection samples of employees appointed during the assurance period that the relevant employees have been introduced to the IT security instructions and, consequently, to the procedures for data processing.	We have noted, on a sample basis, that not all employees have been introduced to the IT security instructions and, consequently, to the procedures for data processing. No further exceptions noted.
C.5	For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned.	Inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal and that assets such as access cards, computers, mobile phones, etc. are returned. Checked by way of inspection of samples of employees resigned or dismissed during the assurance period that rights have been deactivated or terminated and that assets have been returned.	No exceptions noted.
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	Checked by way of inspection that formalised procedures exist to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality. Checked by way of inspection of employees resigned or dismissed during the assurance period that documentation exists for the continued validity of the confidentiality agreement and the general duty of confidentiality.	No exceptions noted.

No.	Novicell's control activity	Deloitte's test	Result of test
C.7	Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data.	Checked by way of inspection that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data.	We have noted that no sufficient awareness training for employees covering general IT security and security of processing related to personal data have been performed. No further exceptions noted.

Control objective D: Procedures and controls are complied with to ensure that personal data can be deleted or returned if arrangements are made with the data controller to this effect.

No.	Novicell's control activity	Deloitte's test	Result of test
D.1	Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller. Assessments are made on a regular basis—and at least once a year—to determine whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place for returning and deleting personal data in accordance with the data processor agreement with the data controller. Checked by way of inspection that the procedures are up to date.	No exceptions noted.
D.2	The following specific requirements have been agreed with respect to the data processor's storage periods and deletion routines: • Upon agreement.	Checked by way of inspection that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines. Checked by way of inspection of data processing sessions from the data processor's list of processing activities that documentation states that personal data are stored in accordance with the agreed storage periods.	No exceptions noted.
D.3	Upon termination of the processing of personal data for the data controller, the data have, in accordance with the agreement with the data controller, been: • Returned to the data controller; and/or • Deleted, provided this is not in conflict with other legislation.	Checked by way of inspection that formalised procedures are in place for processing the data controller's data upon termination of personal data processing. Checked by way of inspection of 5 terminated data processing sessions during the assurance period that documentation exists that the agreed deletion or return of data has taken place.	No exceptions noted.

Control objective E: Procedures and controls are complied with to ensure that the data processor will only store personal data in accordance with the agreement with the data controller.

No.	Novicell's control activity	Deloitte's test	Result of test
E.1	Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller. Assessments are made on a regular basis—and at least once a year—to determine whether the procedures should be updated.	Checked by way of inspection that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements. Checked by way of inspection that the procedures are up to date. Checked by way of inspection of samples of data processing agreements that documentation exists that data are only stored in accordance with the agreement with the data controller.	No exceptions noted.
E.2	Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.	Checked by way of inspection that the data processor has a complete and up-to-date list of processing activities stating localities, countries, or regions. Checked by way of inspection of samples of data processing sessions from Novicell's list of processing activities that documentation exists that the processing of data, including the storage of personal data, takes place only in the localities stated in the data processing agreement—or otherwise as approved by the data controller.	No exceptions noted.

Control objective F: Procedures and controls are complied with to ensure that only approved sub-processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.

No.	Novicell's control activity	Deloitte's test	Result of test
F.1	Written procedures exist which include requirements for the data processor when using sub-processors, including requirements for sub-data processing agreements and instructions. Assessments are made on a regular basis—and at least once a year—to determine whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place for using sub-processors, including requirements for sub-data processing agreements and instructions. Checked by way of inspection that procedures are up to date.	No exceptions noted.
F.2	The data processor only uses sub-processors to process personal data that have been specifically or generally approved by the data controller.	Checked by way of inspection that the data processor has a complete and up-to-date list of sub-processors used. Checked by way of inspection of samples of sub-processors from the data processor's list that documentation exists confirming that the processing of data by the sub-processors is specified in the data processing agreements or otherwise approved by the data controller.	No exceptions noted.
F.3	When changing the generally approved sub-processors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the data processor. When changing the specially approved sub-processors used, this has been approved by the data controller.	Checked by way of inspection that formalised procedures are in place for informing the data controller when changes are made as to the sub-processors used. Checked by way of inspection that the data controller was informed when changing the sub-data processor used throughout the assurance period.	No exceptions noted.
F.4	The data processor has subjected the sub-processor to the same data protection obligations as those set out in the data processing agreement or a similar document with the data controller.	Checked by way of inspection that sub-data processing agreements have been entered into with sub-processors used. Checked by way of inspection of samples of sub-data processing agreements that they include the	No exceptions noted.

No.	Novicell's control activity	Deloitte's test	Result of test
		same requirements and obligations as those stated in the data processing agreements between the data controllers and the data processor.	
F.5	The data processor has a list of approved sub-processors disclosing: • Name • Business registration no. • Address • Description of the processing.	Checked by way of inspection that Novicell has a complete and up-to-date list of sub-processors used and approved. Checked by way of inspection that the list does include all the required details about each sub-data processor.	We have noted that the list of approved sub-processors does not include the required details about each sub-data processor. No further exceptions noted.
F.6	Based on an updated risk assessment of each sub-data processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the sub-data processor.	Checked by way of inspection that formalised procedures are in place for following up on processing activities at sub-processors, and checked their compliance with the sub-data processing agreements. Checked by way of inspection of samples of sub-processors that the current processing activities at such sub-processors are subjected to risk assessment. Checked by way of inspection of samples of technical and organisational measures that security of processing at the sub-processors used, and similar matters, are appropriately followed up.	No exceptions noted.

Control objective G: Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.

No.	Novicell's control activity	Deloitte's test	Result of test
G.1	Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Assessments are made on a regular basis—and at least once a year—to determine whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place to ensure that personal data are only transferred to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Checked by way of inspection that procedures are up to date.	No exceptions noted.
G.2	The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.	Checked by way of inspection that the data processor has a complete and updated list of transfers of personal data to third countries or international organisations. Checked by way of inspection that the data processor has a complete and updated list of transfers of personal data to third countries or international organisations.	No exceptions noted.
G.3	As part of the transfer of personal data to third countries or international organisations, the data processor assessed and documented the existence of a valid basis of transfer.	Checked by way of inspection that formalised procedures are in place for ensuring a valid basis of transfer. Checked by way of inspection that procedures are up to date. Checked by way of inspection of a sample of data transfers from the data processor's list of transfers that documentation confirms a valid basis for transfer in the data processing agreement with the data controller, and that transfers have only taken place insofar as they were agreed with the data controller.	No exceptions noted.

Control objective H: Procedures and controls are complied with to ensure that the data processor can assist the data controller in handing out, correcting, deleting or restricting information on the processing of personal data to the data subject.

No.	Novicell's control activity	Deloitte's test	Result of test
H.1	Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects. Assessments are made on a regular basis—and at least once a year—to determine whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place for the data processor's assistance to the data controller regarding the rights of data subjects. Checked by way of inspection that procedures are up to date.	No exceptions noted.
H.2	The data processor has established procedures, insofar as this was agreed, to enable timely assistance to the data controller in providing, correcting, deleting, restricting, or supplying information about the processing of personal data to data subjects.	Checked by way of inspection that the procedures in place for assisting the data controller include detailed steps for: • Providing data • Correcting data • Deleting data • Restricting the processing of personal data • Providing information about the processing of personal data to data subjects. Checked by way of inspection that the applications support the performance of the relevant detailed procedures.	No exceptions noted.

Control objective I: Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.

No.	Novicell's control activity	Deloitte's test	Result of test
I.1	Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches. Assessments are made on a regular basis—and at least once a year—to determine whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. Checked by way of inspection that procedures are up to date.	No exceptions noted.
I.2	The data processor has established the following controls to identify any personal data breaches: • Awareness of employees • Monitoring of network traffic • Follow-up on logging of access to personal data.	Checked by way of inspection that the data processor provides awareness training to the employees in identifying any personal data breaches. Checked by way of inspection that network traffic is monitored and that anomalies, monitoring alarms, large file transfers, and similar events are appropriately followed up. Checked by way of inspection that logging of access to personal data has been established.	We have noted that insufficient awareness training for employees covering general IT security, and the security of processing related to personal data has been performed. We have noted that there are no written procedures for setting up logging of user activities in systems, databases, or networks used to process and transmit personal data. No further exceptions noted.
I.3	If any personal data breach occurred, the data processor informed the data controller without undue delay and no later than 72 hours after becoming aware of such a breach at the data processor or a sub-processor.	Made inquiries of the sub-processors and Novicell as to whether they have identified any personal data breaches throughout the assurance period.	No exceptions noted.
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency. These procedures must contain instructions on descriptions of: • The nature of the personal data breach • Probable consequences of the personal data breach	Checked by way of inspection that the procedures in place for informing the data controllers in the event of any personal data breach include detailed procedures for: • Describing the nature of the personal data breach;	No exceptions noted.

No.	Novicell's control activity	Deloitte's test	Result of test
	• Measures taken or proposed to be taken to respond to the personal data breach.	• Describing the probable consequences of the personal data breach; • Describing the measures taken or proposed to be taken to respond to the personal data breach. Checked by way of inspection that the procedures available support the measures taken to respond to the personal data breach.	

Section 5: Additional information provided by Novicell ApS

The information contained in this Section 5 has been prepared by Novicell ApS to provide additional information to the customers. The section is not to be considered part of the system description. The information in Section 5 is not covered by Deloitte's procedures that intend to assess whether the system description is accurate; whether controls that support the control objectives in Section 4 have been appropriately designed; and whether the controls have functioned effectively during the period. Thus, Deloitte's conclusion does not include the information in this section.

Novicell ApS management's response to the noted deviations

No.	Novicell's control activity	Result of test	Management's response
A.1	Written procedures are in place which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis - and at least once a year - to determine whether the procedures need updating.	We have noted that the security committee's annual review of written procedures was conducted outside the assurance period. No further exceptions noted.	Novicell has established written procedures ensuring that personal data is only processed on documented instructions from the data controller and in accordance with the applicable data processing agreements. All agreements are reviewed at least annually to ensure they remain accurate, complete, and compliant. This ensures ongoing oversight and control over personal data processing. Novicell has a formalized procedure in place to review its IT security policy on an annual basis. This review is conducted as part of a recurring security governance meeting. The latest review was completed shortly after the end of the assurance period, ensuring that policies and procedures remain current and aligned with applicable requirements.
B.1	Written procedures exist that include a requirement for safeguards to be established for the processing of personal data in accordance with the agreement with the data controller. Assessments are made on a regular basis - and at least once a year - to determine whether the procedures should be updated	We have noted that the security committee's annual review of written procedures was conducted outside the assurance period. No further exceptions noted.	Novicell has a formalized procedure in place to review its IT security policy on an annual basis. This review is conducted as part of a recurring security governance meeting. The latest review was completed shortly after the end of the assurance period, ensuring that policies and procedures remain current and aligned with applicable requirements.
B.6	Access to personal data is isolated to users with a work-related need for such access.	We have noted that there are no formalised procedures in place for restricting users' access to personal data.	Novicell has established controls and workflows for granting and revoking user access to ensure that access to personal data is granted only to employees with a legitimate business need. Access provisioning is managed by IT support based on documented

No.	Novicell's control activity	Result of test	Management's response
		We have noted a lack of management of user lists, which compromises the ability to ensure that access to personal data is appropriately restricted. We have noted, on a sample basis, a lack of functional segregation of duties in one system. We have noted, on a sample basis, that user access review is not effectively conducted. We noted that user access review is not conducted in a timely manner. No further exceptions noted.	requests and approvals from relevant team leads or project managers, with all processes tracked and monitored in systems such as Jira. Regular user access reviews are conducted to verify that access rights remain appropriate. These controls and monitoring mechanisms help ensure compliance with data protection requirements. Novicell are internally reviewing opportunities to optimize this process and procedure further.

B.9	Logging of the following matters has been established in systems, databases and networks:
	
	• Activities performed by system administrators and others holding special rights
	• Security incidents comprising:
	  ○ Changes in log setups, including disabling of logging
	  ○ Changes in users' system rights
	  ○ Failed attempts to log on to systems, databases or networks.
	
	Logon data are protected against manipulation and technical errors, and are reviewed regularly.
		We have noted that there are no written procedures for setting up logging of user activities in systems, databases, or networks that are used to process and transmit personal data.
		
		No further exceptions noted.
			Novicell acknowledge this and are currently in the process of conducting an internal review of the documented procedure.

B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to	We have not been able to test the effectiveness of the control due to an insufficient and incomplete overview of personal data used for development, testing, or similar activities.	We acknowledge the observation regarding the oversight of pseudonymisation and anonymisation. Novicell has established procedures to use only anonymised or pseudonymised data in development, testing, and similar non-production activities. Following this

No.	Novicell's control activity	Result of test	Management's response
	accomplish the data controller's purpose according to agreement and on the data controller's behalf.	No further exceptions noted.	audit, Novicell is internally reviewing opportunities to optimise these processes and procedures further to enhance oversight.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	We have noted that there is no established procedure to regularly test technical measures through vulnerability scans or penetration tests. Furthermore, vulnerability scans and penetration tests have not been conducted during the assurance period. No further exceptions noted.	Novicell acknowledge this and will ensure that a formal procedure and test are established and carried out.
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	We have noted that a formalised procedure is not in place for granting and removing users' access to systems and databases used to process personal data. We have noted that there is a lack of management of user lists, which compromises the ability to ensure that access to personal data is appropriately restricted. We have not been able to test the implementation and operating effectiveness of the user provisioning and deprovisioning controls, as we were unable to obtain a complete list of user creations and deletions for the systems. On a sample basis, we have noted a lack of functional segregation of duties in one system. On a sample basis, we have noted that user access reviews are not conducted effectively. We noted that user access review is not conducted in a timely manner.	Novicell has established formal procedures for granting and revoking employee access. Access management is integrated into our on/offboarding system. IT Support coordinating access requests via team leads or managers. Our compliance system includes controls that ensure user access is regularly reviewed, updated, or removed when no longer required. Novicell are internally reviewing opportunities to optimize this process and procedure further.

No.	Novicell's control activity	Result of test	Management's response
		No further exceptions noted.	
B.15	Physical access safeguards have been established so as to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed.	On a sample basis, we noted that monitoring and review of a third-party service provider's assurance report, specifically concerning physical security measures, have not been obtained or performed. No further exceptions noted.	Novicell conducts an annual comprehensive review of all third-party service providers. This review includes a detailed assessment of their assurance reports. Additionally, the process involves verifying applicable certifications and reviewing data processing agreements to ensure compliance with security and privacy requirements. Evidence of these reviews, including assessments and confirmations, was provided and made available during the audit. We acknowledge that, for one third-party supplier, the review did not include a sufficiently detailed assessment of physical security measures. This issue is being addressed and will be strengthened as part of our ongoing efforts to enhance third-party risk monitoring in accordance with our control framework.
C.1	Management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The IT security policy is based on the risk assessment performed. Assessments are made on a regular basis - and at least once a year - to determine whether the IT security policy should be updated.	We have noted that the security committee's annual review of written procedures was conducted outside the assurance period. No further exceptions noted.	Novicell has a formalized procedure in place to review its IT security policy on an annual basis. This review is conducted as part of a recurring security governance meeting. The latest review was completed shortly after the end of the assurance period, ensuring that policies and procedures remain current and aligned with applicable requirements.
C.3	The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant: • References from former employers • Diplomas.	We have noted that references from former employers or diplomas are not obtained consistently. No further exceptions noted.	At Novicell, the recruitment process follows a clear and established procedure. This includes collecting CVs and job applications as part of the candidate evaluation. References from former employers or diplomas are not routinely required but may be requested in specific cases where relevant and with the candidate's consent.

No.	Novicell's control activity	Result of test	Management's response
C.4	Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.	We have noted, on a sample basis, that not all employees have been introduced to the IT security instructions and, consequently, to the procedures for data processing. No further exceptions noted.	At Novicell, an established procedure is in place to inform new employees about data processing and IT security practices upon hiring. Each year, managers receive the updated security policy, which they are responsible for communicating to their teams, ensuring employees are made aware of the relevant guidelines and requirements. Additionally, all policies are accessible on the company intranet, allowing employees to review and reference them at any time. Following this audit, additional emphasis has been placed on ensuring that all employees are introduced to the relevant IT security instructions and procedures.
C.7	Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data.	We have noted that no sufficient awareness training for employees covering general IT security and security of processing related to personal data have been performed. No further exceptions noted.	At Novicell, there is a clear and established procedure in place for informing new employees about data processing and IT security practices upon hiring. Each year, managers receive the updated security policy, which they are responsible for communicating to their teams, ensuring that employees are made aware of relevant guidelines and requirements. Additionally, all policies are accessible on the company intranet, allowing employees to review and reference them at any time. Novicell acknowledges the lack of ongoing awareness during the assurance period. Increased focus has been placed on ongoing awareness training, which now has been established and implemented after the assurance period. These measures ensure that employees are regularly made aware of applicable data protection and security requirements - both at the time of hiring and on an ongoing basis.
F.5	The data processor has a list of approved sub-processors disclosing: • Name • Business registration no. • Address	We have noted that the list of approved sub-processors does not include the required details about each sub-data processor. No further exceptions noted.	Novicell maintains a complete and up-to-date list of approved sub-processors, which includes all required details such as name, business registration no., address, description.

No.	Novicell's control activity	Result of test	Management's response
	• Description of the processing.		During the assurance period, Novicell transitioned to a new compliance system, which may have temporarily impacted the visibility of certain information. However, all data has since been reviewed, updated, and properly entered for each sub-processor to ensure full compliance.
I.2	The data processor has established the following controls to identify any personal data breaches: • Awareness of employees • Monitoring of network traffic • Follow-up on logging of access to personal data.	We have noted that insufficient awareness training for employees covering general IT security and the security of processing related to personal data has been performed. We have noted that there are no written procedures for setting up logging of user activities in systems, databases, or networks used to process and transmit personal data. No further exceptions noted.	At Novicell, new employees are introduced to data protection and IT security practices as part of the onboarding process. All relevant policies are accessible via the company intranet, and managers are responsible for communicating updates to their teams. Furthermore, ongoing awareness training has been established and implemented following the assurance period to ensure continuous employee awareness of data protection and security requirements. Novicell acknowledges the observation regarding documented procedures for logging. We have implemented logging of user activities across our internal and external domain controllers, as well as in Microsoft Entra ID. We are currently reviewing our internal documentation to establish a clear procedure for logging.

The signatures in this document are legally binding. The document is signed using Penneo™ secure digital signature. The identity of the signers has been recorded, and are listed below.

"By my signature I confirm all dates and content in this document."

Kristian Kjærgaard Rasmussen
Intern underskriver
Serial number: 40b1a381-eb14-4aa1-9108-8d12b2625fd4
IP: 93.178.xxx.xxx
2025-11-25 11:27:05 UTC

Michael Daugaard Bagger
DELOITTE STATSAUTORISERET REVISIONSPARTNERSELSKAB
CVR: 33963556
Ekstern underskriver
Serial number: bbca224f-0d8f-4364-90a3-806dbf38c9b6
IP: 163.116.xxx.xxx
2025-11-25 13:17:16 UTC

Thomas Kühn
Ekstern underskriver
Serial number: d1fc228f-48ef-4abe-abad-efe9492b4894
IP: 93.164.xxx.xxx
2025-11-27 07:03:22 UTC