# cBrain A/S

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with the data controllers using F2 and M4 systems for the period 1 January 2025 to 31 December 2025.

## Content

# 1 Management's statement

cBrain A/S (hereafter cBrain) processes personal data for data controllers in accordance with the data processing agreement.

The accompanying Description has been prepared for data controllers, who have used F2- and M4-systems, and who have a sufficient understanding to consider the description along with other information, including information about controls operated by subservice organizations and the data controllers themselves in assessing whether the requirements of the EU Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "the Regulation") have been complied with.

cBrain uses a subservice organization to Sentia in connection with the delivery of hosting services. The Description includes only the control objectives and related controls of cBrain and excludes the control objectives and related controls of the subservice organization. Certain control objectives specified in the Description can be achieved only if subservice organization controls assumed in the design of our controls are suitably designed and operating effectively. The Description does not extend to controls of the subservice organization.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of cBrain's controls are suitably designed and operating effectively, along with related controls at the data processor. The Description does not extend to controls of the data controller.

cBrain confirms that:

a) The accompanying description in section 3, fairly presents the functions performed by the F2- and M4-systems, which have processed personal data for data controllers subject to the Regulation throughout the period from 1 January 2025 to 31 December 2025. The criteria used in making this statement were that the accompanying description:

   (i) Presents how the functions performed by the F2- and M4-systems were designed and implemented, including, if applicable:

      I. The types of services provided, including the type 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 procedures supporting in the event of breach of personal data security that the data controller may report this to the supervisory authority and inform the data subjects

      VII. The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

      VIII. Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.

      IX. Controls that we, in reference to the scope of F2 and M4 systems, have assumed would be implemented by the data controllers and which, if necessary, in order to

achieve the control objectives stated in the Description, are identified in the Description

X. 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

(ii) Includes relevant information of changes in information security and measures in relation to F2 and M4 systems processing of personal data in the period from 1 January 2025 to 31 December 2025.

(iii) Does not omit or distort information relevant to the scope of information security and measures in relation to F2- and M4-systems being 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 information security and measures in relation to F2- and M4-systems that the individual data controllers might consider important in their particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 January 2025 to 31 December 2025 , if controls at subservice organizations were suitably designed and operating effectively, and data controller applied the complementary user entity controls assumed in the design of cBrain's controls throughout the period from 1 January 2025 to 31 December 2025. The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved and

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 January 2025 to 31 December 2025

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

Copenhagen, 26. February 2026
cBrain A/S

Ejvind Jørgensen
Market Director

# 2 Independent service auditor's report

**Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with the data controllers using F2 and M4 systems for the period 1 January 2025 to 31 December 2025.**

To: cBrain and data controllers using F2 and M4 systems

## Scope

We have been engaged to provide assurance about cBrain's Description in section 3 of information security and measures in relation to F2 and M4 systems in accordance with the data processing agreement with data controllers throughout the period from 1 January 2025 to 31 December 2025 ("the Description") and about the design and operating effectiveness of controls related to the control objectives stated in the Description. We express reasonable assurance in our conclusion.

The Description indicates that certain control objectives can only be achieved if the complementary user entity controls assumed in the design of cBrain's controls are suitably designed and operating effectively, along with related controls at cBrain. Our engagement did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

cBrain uses Sentia in connection with the delivery of hosting services. The Description includes only the control objectives and related controls of cBrain and excludes the control objectives and related controls of Sentia. Certain control objectives specified by cBrain can be achieved only if subservice organization controls assumed in the design of cBrain's controls are suitably designed and operating effectively, along with the related controls at cBrain. Our engagement did not extend to controls of Sentia and we have not evaluated the suitability of the design or operating effectiveness of such subservice organization controls.

## cBrain's responsibilities

cBrain is responsible for: preparing the Description and the accompanying statement in section 1, including the completeness, accuracy, and the method of presentation of the Description and statement, providing the services covered by the Description; stating the control objectives; identifying the risks that threaten the achievement of the control objectives; selecting the criteria presented in the statement; and designing, implementing and effectively operating controls to achieve the stated control objectives.

## Our independence and quality control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour as well as ethical requirements applicable in Denmark.

EY Godkendt Revisionspartnerselskab applies International Standard on Quality Management 1, ISQM 1, which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

## Our responsibilities

Our responsibility is to express an opinion on cBrain's Description and on the design and operating effectiveness of controls related to the control objectives stated in that Description, based on our procedures. 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, 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 suitably designed and operating effectively.

An assurance engagement to report on the Description, design, and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data

processor's description of its information security and measures in relation to F2 and M4 systems and about the design and operating effectiveness of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved.

An assurance engagement of this type also includes evaluating the overall presentation of the Description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the data processor and described in section 1.

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

### Limitations of controls at a data controller

cBrain's Description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the standard applications F2 and M4 systems that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect all personal data breaches. Furthermore, the projection of any evaluation of the operating effectiveness to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

### 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 Section 1 "Management's statement". In our opinion, in all material respects:

(a) The Description fairly presents information security and measures in relation to F2 and M4 systems as designed and implemented throughout the period from 1 January 2025 to 31 December 2025

(b) The controls related to the control objectives stated in the Description were suitably designed throughout the period from 1 January 2025 to 31 December 2025 to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period 1 January 2025 to 31 December 2025, if relevant controls at subservice organisations and complementary controls at data controllers are suitably designed and implemented throughout the period 1 January 2025 to 31 December 2025 as assumed in the design of cBrain's controls 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 January 2025 to 31 December 2025, if relevant controls at subservice organisations are operating effectively, and complementary user entity controls at the data controller assumed in the design of cBrain's controls operated effectively throughout the period 1 January 2025 to 31 December 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 and the description of tests of controls in section 4 are intended only for data controllers who have used cBrain's F2 and M4 systems, who have a sufficient understanding to consider it along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the Regulation have been complied with.

Copenhagen, 26 February 2026
EY Godkendt Revisionspartnerselskab
CVR no. 30 70 02 28

Jesper Due Sørensen
Partner

Jan K. Mortensen
statsaut. revisor
mne40030

# 3 Process description

cBrain A/S is the provider of the F2 and M4 solutions with associated services for cBrain's customers.

The solutions support customers in a range of digital business processes involving employees, members, citizens, authorities, and companies. The solutions are implemented in organizations in both the private and the public sector. The digital business processes include case and document management, business critical processes, membership management, booking of meetings, management support, subsidy administration, rulings, approvals, etc. Customers are located in Denmark and internationally.

Services related to digitalization can be both consultancy services and services involving the delivery of software.

In relation to data processing, a range of services do not entail cBrain acting as the data processor, e.g. certain consultancy tasks such as counselling, training, workshops, design tasks, and architectural tasks. There are also software services which do not involve cBrain as the data processor, e.g. developing a proof of concept or installing a test system.

## 3.1 Process characterization

When cBrain is the data processor, its services are characterized by cBrain acting as:

- operations provider
- support provider
- ad hoc task provider.

### 3.1.1 cBrain is the operations provider

This service is provided to customers with a hosting agreement or cloud agreement and who are located in cBrain's operation environment at Sentia. In this instance, it is cBrain's responsibility to ensure that operations are carried out as per the agreed-upon service level agreement and security requirements.

### 3.1.2 cBrain is the support provider

All customers have a software maintenance agreement which grants them access to support services. In connection with performing support services, cBrain has access to customers' systems and data. Data access and thus data processing is solely for resolving the customer's problem or question related to the software covered by the software maintenance agreement. Software errors are resolved through new software releases.

### 3.1.3 cBrain is the ad hoc task provider

Agreements regarding the delivery of tasks may be part of a customer's initial go-live delivery agreement or the subsequent collaboration where the customer wishes additional deliveries. Additional deliveries are subject to the delivery contract and are designated change requests. Tasks which include cBrain's processing of data include:

- data conversion
- upgrading
- submissions to the National Archives or a similar institution
- database relocation
- database update.

The general terms regarding data processing and instructions are stated in the data processor agreements. As a rule, cBrain only performs data processing for customers with a data processor agreement. Furthermore, cBrain has introduced additional specifications regarding instructions for carrying out ad hoc tasks. These are in place to make relevant employees at the customer and at cBrain aware of the instructions pertaining to a given task.

## 3.2 Personal data

The customer's application of the software entails the processing of sensitive personal data.

The types of sensitive personal data include:

- general personal data including identification details such as name and address or information about finances, tax, debt, significant social issues, other private matters, sick days, official matters, family matters, housing, car, education, exams, job applications, CV, employment date and position, work area, and work phone
- special categories of personal data, including race and ethnic origin, trade union membership, and health information
- other personal data, including information about criminal offenses and social security number.

Categories of registered individuals covered by the data processor agreement:

- employees
- citizens
- foreign citizens (for example people who are working or studying in Denmark or applying for citizenship)
- individuals associated with companies.

## 3.3 Practical measures

A well-documented control apparatus has been established to support data processing security for the three main services of operations, support, and ad hoc tasks, respectively.

cBrain has organized the IT security based on ISO 27001. Processes related to the F2 product and employees employed in Denmark are ISO 27001 certified.

Employees are subject to confidentiality agreements, and processes for onboarding, offboarding, and reboarding have been established to ensure that access conditions, etc., correspond to employment conditions. A large number of cBrain's employees have security clearance for working with customers in the public sector. Ongoing awareness training is carried out to ensure that employees are continuously updated on security measures and processes.

Software development is carried out by employees at cBrain in Denmark, and the support systems used for software maintenance and support requests are also operated and maintained by cBrain employees in Denmark.

Standards are devised for security measures in relation to data access control and security levels, which are implemented in collaboration with the customer. Control measures and reporting are in place for when the customer deviates from the recommended procedure.

Standard operating procedures (SOPs) exist for a range of activities, including personally identifiable data in connection with support reporting. Protocols are in place for what is allowed and how and when data from support systems are deleted.

## 3.4 Use of subcontractors

cBrain uses Sentia as a partner for providing hosting services.

Sentia is a full-service hosting company. The company delivers professional IT solutions to public and private companies. Its services include virtual solutions, colocation (physical racks), operations solutions and outsourcing, backup (including remote backup), storage, professional Internet connections, IP traffic, and a secure environment. Sentia operates data centers in Denmark which are redundantly connected and connected to Denmark's largest telecommunication hubs.

In their collaboration with cBrain, Sentia only delivers the physical infrastructure for hosting, while cBrain owns and manages the hardware and software, including basic software, databases, etc. Only

specific cBrain employees can access cBrain's servers in Sentia's locations in Denmark. Customer data, including backup, is located in Denmark.

Sentia's administrative personnel do not have access to connect to cBrain's servers. For support purposes, to ensure maximum uptime and potential troubleshooting, Sentia has administrative rights to the firewall in Taastrup. It has been assessed that Sentia is not a sub processor, as Sentia does not have server access and therefore cannot access data.

The IT security at Sentia is verified by having an independent third party to prepare ISAE 3000 and 3402 reports each year. Their ISAE reports are subsequently reviewed and approved at cBrain. Note that this ISAE report does not include services delivered by Sentia.

By owning the servers, etc., which are located both at Sentia and in cBrain's offices, cBrain ensures that individuals or organizations from safe/unsafe third countries do not have access to process data, e.g. in relation to support services (this also applies to "view access") or development.

To access cBrain's offices in Denmark, an access chip and a code are required to enter the server room. Access to the office premises requires an access chip during office hours and an access chip and a code outside of office hours.

## 3.5 Risk assessment

cBrain conducts a risk assessment at least once a year. The assessment is based on KOMBIT's standard for risk assessment. The assessment itself is based on a number of potential events involving the risk of confidentiality loss, integrity loss, and availability loss. For each of these, an assessment is made of the likelihood of the event and its consequences (for the registered individual, reputation, financial, etc.).

cBrain holds quarterly Management Review meetings to address compliance with ISO 27001. Management Review meetings are an ISO 27001 requirement.

## 3.6 Processes regarding personal data

Processes in both IT and manual systems used to initiate, register, process, and if necessary, correct, delete, and restrict the processing of personal data.

All processing of personal information in customer data must follow a set of instructions.

Instructions can be expressed in relation to the following:

- Delivery agreements
- Hosting agreements
- Software maintenance
- Support
- Ad hoc tasks or individual tasks such as upgrading, integration, submission.

Instructions are regulated by the data processor agreement entered into with the customer. The instructions include initiation, registration, processing including limitations, correction, and deletion of personal data.

All standard services related to GDPR (personal data processing) are approved by a member of the Management Group to ensure compliance with current legislation.

cBrain carries out an assessment in the event of changes in legislation or if new guidelines are issued by the Danish Data Protection Agency or by KOMBIT in relation to data processor agreements.

All incidents that have been assessed as in violation of legislation must be reported to the data controller.

Processes which upon termination of data processing ensure that, according to the data controller's choice, all personal data is deleted or returned to the data controller, unless legislation or regulation requires the retention of personal data.

Procedures for data management in the event of termination apply to customers whose activities are located in cBrain's hosting center.

cBrain provides data to the customer in cBrain-hosted F2 and M4 systems in connection with customer exit, in accordance with the agreement with the customers. The systems, including data, are subsequently deleted as part of the customer offboarding process.

Data in cBrain's support system is continuously deleted. Procedures and guidelines are in place for both customers' and cBrain employees' use of the support system to prevent the use of personal information in support cases.

***Processes which in case of breach of personal data security support the data controller in notifying the supervisory authority as well as informing the data subjects.***

cBrain's procedure for handling security breaches includes notifying affected customers about:

a) The character of the security breach

b) Likely consequences of security breaches

c) Measures taken or proposed to handle security breaches.

cBrain has informed us, in its data processor agreements how support is provided to the data controller in relation to the rights of the data subjects. cBrain has a procedure in place to ensure this is handled in accordance with the data processor agreement entered into with the customer.

The procedure enables timely assistance to the data controller in relation to the following:

- Provision of information
- Correction of information
- Deletion of information
- Restriction of processing of personal data
- Disclosure of processing of personal data to the data subject.

***Processes which ensure suitable technical and organizational security measures for the processing of personal data under consideration of the risks posed by processing, especially accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to transmitted, stored or otherwise processed personal data.***

The procedure for establishing security measures is defined by the various instructions.

Instructions can be expressed in relation to the following:

- Delivery agreements
- Hosting agreements
- Software maintenance
- Support (Ad hoc tasks)
- Individual solution descriptions (upgrading, integration, submission).

cBrain has implemented standard operating procedures for tasks and devised procedures related to ISO 27001.

Risk assessment is conducted annually for the company, including for F2, M4, and suppliers. Revaluation and recapitulation of risk assessments occur continuously at Management Review meetings.

cBrain has implemented IT security and GDPR policies. New cBrain employees receive training in IT security at the start of employment, and annual refresher training is conducted for all employees. cBrain employees are subject to confidentiality provisions, both during and after their employment at cBrain.

cBrain enters into data processor agreements with customers and suppliers to the extent necessary. It is verified annually that the company's data processor agreements are in accordance with IT security and GDPR policies.

## 3.7 Control measures

A range of control measures have been implemented, part of which are recommended for the protection of personal data, and part of which are recommended in relation to ISO 27001 activities. Control measures are continuously adjusted and revised in relation to risk assessment and general changes in market conditions.

Refer to section 4, in which the specific control activities are described.

## 3.8 Complementary controls by the data controllers

The data controller has the following obligations:

- The data controller must ensure at all times that the given instructions are comprehensive for the processing of personal information which is carried out by cBrain on behalf of the data controller, and that the processing is in accordance with the current special legislation and data protection laws and regulations.
- cBrain can set up audit logging in the systems after prior consent from the customer. It is the customer's responsibility to consider the logging requirements set up in the user interface of F2 and M4. It is also the customer's responsibility that logs are regularly reviewed. Only the administrator role at the customer, who can access the audit log.
- F2 and M4 customers are responsible for assigning employees roles which provide different levels of access to the solution. It is the responsibility of the customer to ensure that only the relevant employees and cBrain employees are granted access at an appropriate level.
- Each customer has access to a test environment and a production environment, which are separate installations and customer exclusive. It is the responsibility of the customer to ensure that data in the test environment does not include the data of real individuals.
- It is the task of the data controller to implement controls for managing user access and rights in F2 and M4.
- The data controller must ensure that personal information in F2 and M4 is deleted in accordance with the current legislation.
- The data controller must ensure that they meet the responsibility specified in the data processor agreement, including notification in the event of a data security breach.

# 4 Control objectives, control activity, tests and test results

## 4.1 Purpose and scope

Our work was performed in accordance with ISAE 3000, Assurance Engagements other than audits or reviews of historical financial information.

Our test of the controls' design and implementation comprised the control objective and related controls, which have been selected by Management and which are stated below. Any other control objectives, related controls and controls at cBrain are not covered by our tests.

The tests performed in connection with the determination of design and operating effectiveness of controls are outlined below.

## 4.2 Tests performed

Below, we have summarised the tests performed by EY in order to assess controls relevant to cBrain's information security and measures pursuant to the data processing agreement:

| | |
|---|---|
| **Inspection** | Reading of documents and reports which contain disclosure on the performance of the control. This work includes i.a. the reading of and position-taking to reports and other documentation to assess whether specific controls have been designed in a way that allow them to be effective, if implemented. Furthermore, we assess whether controls are adequately monitored at suitable intervals.<br>As to the technical platforms, databases and network components, we tested the specific system set-up to ensure that controls were designed, implemented and operating effectively throughout the period 1 January 2025 to 31 December 2025. |
| **Inquiry** | Inquiries of suitable staff with cBrain. Inquiries comprised i.a. the performance of controls. |
| **Observation** | We observed the performance of controls. |

## 4.3 Control objectives, control activity, tests and results

| **Control objective A**<br>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.* | *cBrain's control activity* | *Test performed by EY* | *Results of auditor's test* |
| A.1 | Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available.<br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | Inspected that formalized procedures exist to ensure that personal data are only processed according to instructions.<br>Inspected that the procedures include a requirement to assess at least once a year the need for updates, including in case of changes in the data controller's instructions or changes in the data processing.<br>Inspected that procedures are up to date. | No deviations noted. |
| A.2 | cBrain only processes personal data stated in the instructions from the data controller. | Inspected that Management ensures that personal data are only processed according to instructions.<br>Inspected of a sample of personal data processing operations that these are conducted consistently with instructions. | No deviations noted. |
| A.3 | cBrain immediately informs the data controller if an instruction, in the cBrain's opinion, infringes the Regulation or other European Union or member state data protection provisions. | Inspected that formalized procedures exist ensuring verification that personal data are not processed against the Regulation or other legislation.<br>Inspected that procedures are in place for informing the data controller of cases where the processing of personal data is evaluated to be against legislation.<br>Inquired if cBrain has registered cases where the processing of personal data was evaluated to be against legislation. Inspected list of incidents. | cBrain has informed that there have been no cases during the assurance period where the processing of personal data was evaluated to be against legislation.<br>No deviations noted. |

| Control objective B<br>Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| *No.* | *cBrain's control activity* | *Test performed by EY* | *Result of auditor's test* |
| B.1 | Written procedures exist which include a requirement that safeguards agreed are established for the processing of personal data in accordance with the agreement with the data controller.<br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | Inspected that formalized procedures exist to ensure establishment of the safeguards agreed.<br>Inspected that procedures are up to date. | No deviations noted. |
| B.2 | cBrain 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. | Inspected that formalized procedures are in place to ensure that cBrain performs a risk assessment to achieve an appropriate level of security.<br>Inspected that the risk assessment performed is up to date and comprises the current processing of personal data.<br>Inspected that cBrain has implemented the technical measures ensuring an appropriate level of security consistent with the risk assessment. | No deviations 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. | Inspected the procedures for the prevention and detection of an outbreak of malicious code and reestablishment after a malicious virus attack.<br>Inspected sample basis that, for the systems and databases used in the processing of personal data, antivirus software has been installed and up to date. | No deviations noted. |
| B.4 | External access to systems and databases used in the processing of personal data takes place through a secured firewall. | Inspected the network diagrams for cBrain and Sentia showing that external access to systems and databases used in the processing of personal data takes place only through a secured firewall. | No deviations noted. |

| Control objective B<br>Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| *No.* | *cBrain's control activity* | *Test performed by EY* | *Result of auditor's test* |
| | | On a sample basis, inspected the implementation of firewall rule controls. | |
| B.5 | Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. | Inspected network diagrams showing the appropriate segmentation at cBrain. | No deviations noted. |
| B.6 | Access to personal data is isolated to users with a work-related need for such access. | Inspected the procedure for registration and de-registration of users.<br>On a sample basis, inspection of users who joined and left during the assurance period to determine whether procedures for user creation and deletion were followed.<br>On a sample basis, inspected if privileged users had a work-related need for access.<br>Inspected the procedure for annual evaluation of administrative access rights.<br>Inspected that an annual review of administrative users has been carried out for AD administrator rights as well as cBrain's internal F2 administrators. | No deviations noted. |
| B.7 | For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. | Inspected the procedure for collection and assessment of technical vulnerabilities.<br>On a sample basis, it was inspected that monitoring with alarms has been set up, including that appropriate measures are implemented to manage the associated risk. | For 4 customers, F2 was open to TLS 1.0 and TLS 1.1 traffic from November 19 to December 31, 2025.<br>For 1 customer, F2 was open to TLS 1.0 and TLS 1.1 traffic from December 3 to December 31, 2025. |

| Control objective B<br>Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| *No.* | *cBrain's control activity* | *Test performed by EY* | *Result of auditor's test* |
| | | | In all cases, TLS 1.0 and TLS 1.1 were disabled during the service window on February 8, 2026.<br>No further deviations noted. |
| B.9 | Relevant security-related actions are logged based on risk assessment and technical proportionality.<br>Microsoft's security baseline is applied, and risk-relevant incidents are logged.<br>Activities performed by system administrators and operators are logged.<br>Logging facilities and log information are protected against manipulation and unauthorized access. | Inspected, for a sample of servers, that logging is carried out in accordance with Microsoft Baseline Recommendations.<br>Inspected the procedure for protecting logging facilities and logs.<br>On a sample basis, it was inspected that logging information from cBrains Windows AD is protected against manipulation and unauthorized access.<br>Inspected procedures for logging activities performed by system administrators and operators.<br>On a sample basis, it was inspected that log configuration on servers to determine whether actions by system administrators and operators are logged. | No deviations noted. |
| B.11 | The technical measures established are tested on a regular basis through vulnerability scans. Vulnerability scans are performed quarterly, commencing in the third quarter of 2025 (2025 Q3). | Inspected that formalized procedures exist for regularly testing technical measures, including for performing vulnerability scans.<br>On a sample basis, it was inspected that monitoring with alarms has been set up, including that appropriate measures are implemented to manage the associated risk. | For 4 customers, F2 was open to TLS 1.0 and TLS 1.1 traffic from November 19 to December 31, 2025.<br>For 1 customer, F2 was open to TLS 1.0 and TLS 1.1 traffic from December 3 to December 31, 2025. |

| Control objective B<br>Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| *No.* | *cBrain's control activity* | *Test performed by EY* | *Result of auditor's test* |
| | | | In all cases, TLS 1.0 and TLS 1.1 were disabled during the service window on February 8, 2026.<br>No further deviations 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 | Inspected that formalized procedures exist for handling changes to systems, databases or networks, including handling of relevant updates, patches and security patches.<br>On a sample basis, it was inspected that servers and databases are timely patched during the assurance period.<br>Inquired if changes have occurred to M4 systems during the assurance period.<br>Inspected the list of changes in the case management system. | cBrain has informed that no changes have been made to M4 system during the assurance period.<br>No deviations noted. |
| B.13 | A formalized procedure is in place for granting and removing users' access to personal data.<br>Privileged users' access is reconsidered annually, including the continued justification of rights by a work-related need. | Inspected that formalized procedures exist for granting and removing users' access.<br>Inspected sample basis employees' access to systems and databases that the user accesses granted have been authorized and that a work-related need exists.<br>Inspected sample basis resigned or dismissed employees that their access to systems and databases was deactivated or removed on a timely basis. | No deviations noted. |

| Control objective B<br>Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| *No.* | *cBrain's control activity* | *Test performed by EY* | *Result of auditor's test* |
| | | Inspected that documentation exists that privileged user accesses granted are evaluated and authorized annually. | |
| B.15 | Physical access safeguards have been established so as to only permit physical access by authorized persons to premises and data centers at which personal data are stored and processed. | Inspected that formalized procedures exist to ensure that only authorized persons can gain physical access to premises and data centers at which personal data are stored and processed.<br>Inspected documentation that, throughout the assurance period, only authorized persons have had physical access to premises and data centers at which personal data are stored and processed. | No deviations noted. |
| B.16 | A supplier risk assessment is evaluated and updated on an annual basis.<br>Audit report from Sentia is obtained and reviewed, and any relevant reported issues identified in the audit report are recorded and followed up on. | Inspected the procedure for managing the suppliers.<br>Inspected that the audit report from Sentia is obtained and reviewed during the assurance period.<br>Inspected documentation that the supplier risk assessment is evaluated and updated during the assurance period. | No deviations noted. |

| Control objective C<br>Procedures and controls are complied with to ensure that cBrain has implemented organizational measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| *No.* | *cBrain's control activity* | *Test performed by EY* | *Result of auditor's test* |
| C.1 | cBrain's management has approved a written information security policy that has been communicated to all relevant stakeholders, including cBrain's employees. The IT security policy is based on the risk assessment performed.<br>Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated. | Inspected that an information security policy exists that Management has considered and approved within the past year.<br>Inspected documentation that the information security policy has been communicated to relevant stakeholders, including the cBrain's employees. | No deviations noted. |
| C.2 | cBrain's management has checked that the information security policy does not conflict with data processing agreements entered into. | Inspected Management's assessment that the information security policy generally meets the requirements for safeguards and the security of processing in the data processing agreements entered into.<br>Inspected a sample of data processing agreements that the requirements in these agreements are covered by the requirements of the information security policy for safeguards and security of processing. | No deviations noted. |
| C.3 | The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant:<br>• References from former employers<br>• Diplomas | Inspected that formalized procedures are in place to ensure screening of cBrain's employees as part of the employment process.<br>Inspected a sample of employees appointed during the assurance period that documentation exists for the assessment of the screening before the employment. | No deviations noted. |

| Control objective C<br>Procedures and controls are complied with to ensure that cBrain has implemented organizational measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| *No.* | *cBrain's control activity* | *Test performed by EY* | *Result of auditor's 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. | Inspected sample of employees appointed during the assurance period that the relevant employees have signed a confidentiality agreement.<br>Inspected sample of employees appointed during the assurance period that the employees have gone through training in information security policy and procedures for processing data. | No deviations noted. |
| C.5 | For resignation or dismissals, cBrain has implemented a process to endures that user's rights are deactivated or terminated. | Inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal.<br>Inspected a sample of employees resigned or dismissed during the assurance period that rights have been deactivated or terminated. | No deviations 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 cBrain for the data controllers. | Inspected that formalized 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.<br>Inspected a sample of employees resigned or dismissed during the assurance period that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality. | No deviations noted. |
| C.7 | cBrain provides awareness training to cBrains employees in relation to IT security and security of processing personal data | Inspected that cBrain provides awareness training to the employees covering general IT | No deviations noted. |

| Control objective C<br>Procedures and controls are complied with to ensure that cBrain has implemented organizational measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| *No.* | *cBrain's control activity* | *Test performed by EY* | *Result of auditor's test* |
| | annually. Employees are introduced to IT security in connection with their employment process. | security and security of processing related to personal data.<br>Inspected documentation that all employees who have either access to or process personal data have the awareness training provided. The employees who have not completed the annual training are followed up.<br>Inspected sample of employees appointed during the assurance period that the employees have gone through training in information security policy and procedures for processing data. | |

| Control objective D<br>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.* | *cBrain's control activity* | *Test performed by EY* | *Result of auditor's 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.<br><br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | Inspected that formalized procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller.<br><br>Inspected that the procedures are up to date. | No deviations noted. |
| D.2 | The following specific requirements have been agreed with respect to cBrain's storage periods and deletion routines:<br>• For data controllers who have a hosting agreement, the data is stored and processed only within Denmark.<br>• In the event of termination of the services relating to the processing, oblige cBrain to, at the choice of the data controller, to delete or return all personal data to the data controllers, as well as to delete existing copies, unless EU law or national law prescribes the storage of the personal data. | Inspected that the existing procedures for storage and deletion include specific requirements for cBrain's storage periods and deletion routines.<br><br>Inspected on a sample basis that documentation exists for personal data is stored in accordance with the data processing agreement.<br><br>Inquired for a sample of data processing documentation confirming that personal data has been deleted in accordance with the agreed deletion procedures during the assurance period. | cBrain has informed us that there have been no terminated data processing activities during the assurance period. Therefore, we have not been able to test the effectiveness of the control.<br><br>No deviations noted. |
| D.3 | Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been:<br>• Returned to the data controller; and/or<br>• Deleted if this is not in conflict with other legislation. | Inspected that formalized procedures are in place for processing the data controller's data upon termination of the processing of personal data.<br><br>Inquired for a sample of data processing documentation confirming that personal data has been deleted in accordance with the agreed deletion procedures during the assurance period. | cBrain has informed us that there have been no terminated data processing activities during the assurance period. Therefore, we have not been able to test the effectiveness of the control.<br><br>No deviations noted. |

| **Control objective E**<br>Procedures and controls are complied with to ensure that cBrain will only store personal data in accordance with the agreement with the data controller. | | | |
|---|---|---|---|
| ***No.*** | ***cBrain's control activity*** | ***Test performed by EY*** | ***Result of auditor's 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.<br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | Inspected that formalized procedures exist for only storing and processing personal data in accordance with the data processing agreements.<br>Inspected that the procedures are up to date. | No deviations noted. |
| E.2 | Data processing and storage by cBrain must only take place in the localities, countries or regions approved by the data controller. | Inspected that cBrain has a complete and updated list of processing activities stating localities, countries or regions.<br>Inspected a sample of data processing sessions from the data processor'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 deviations noted. |

| **Control objective H**<br>Procedures and controls are complied with to ensure that cBrain can assist the data controller in handing out, correcting, deleting or restricting information on the processing of personal data to the data subject. | | | |
|---|---|---|---|
| *No.* | *cBrain's control activity* | *Test performed by EY* | *Result of auditor's test* |
| H.1 | Written procedures exist which include a requirement that cBrain must assist the data controller in relation to the rights of data subjects.<br><br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | Inspected that formalized procedures are in place for cBrain's assistance to the data controller in relation to the rights of data subjects.<br><br>Inspected that procedures are up to date. | No deviations noted. |
| H.2 | cBrain has established procedures in so far as this was agreed that enable timely assistance to the data controller in handing out, correcting, deleting or restricting or providing information about the processing of personal data to data subjects. | Inspected that the procedures in place for assisting the data controller include detailed procedures for:<br>• Handing out data<br>• Correcting data<br>• Deleting data<br>• Restricting the processing of personal data<br>• Providing information about the processing of personal data to data subjects.<br><br>Inquired if cBrain has obtained requests by the data controller for assistance in handing out, correcting, deleting or restricting or providing information about the processing of personal data to data subjects during the assurance period. | cBrain has informed us that they have not obtained requests by the data controller for assistance in handing out, correcting, deleting or restricting or providing information about the processing of personal data to data subjects during the assurance period.<br><br>No deviations noted. |

| Control objective I<br>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.* | *cBrain's control activity* | *Test performed by EY* | *Result of auditor's test* |
| I.1 | Written procedures exist which include a requirement that cBrain must inform the data controllers in the event of any personal data breaches.<br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | Inspected that formalized procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches.<br>Inspected that procedures are up to date. | No deviations noted. |
| I.2 | cBrain has established the following controls to identify any personal data breaches:<br>• Awareness of employees<br>• Monitoring of network traffic. | Inspected that cBrain provides awareness training to the employees in identifying any personal data breaches.<br>Inspected documentation that network traffic is monitored and that anomalies, monitoring alarms, large file transfers, etc. is followed up on. | No deviations noted. |
| I.3 | If any personal data breach occurred, cBrain informed the data controller without undue delay after having become aware of such personal data breach at cBrain or a sub-data processor. | Inspected that cBrain has a list of security incidents disclosing whether the individual incidents involved a personal data breach.<br>Inspected that cBrain has included any personal data breaches at sub-data processors in cBrain's list of security incidents.<br>Inspected that recorded breaches of personal data at cBrain or subcontractors have been communicated to the affected data controllers without undue delay during the assurance period. | No deviations noted. |

| Control objective I<br>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.* | *cBrain's control activity* | *Test performed by EY* | *Result of auditor's test* |
| I.4 | cBrain has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency<br>• Nature of the personal data breach<br>• Probable consequences of the personal data breach<br>• Measures taken or proposed to be taken to respond to the personal data breach. | Inspected that the procedures in place for informing the data controllers in the event of any personal data breach include detailed procedures for:<br>• Describing the nature of the personal data breach<br>• Describing the probable consequences of the personal data breach<br>• Describing measures taken or proposed to be taken to respond to the personal data breach.<br>Inspected documentation confirming that measures have been taken to address breaches of personal data. | cBrain has informed us that they have not received any requests for assistance during the assurance period regarding the notification of breaches to the Data Protection Agency.<br>No deviations noted. |

*Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.*

*"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."*

**Ejvind Jørgensen**
**Market Director**
*På vegne af: cBrain A/S*
*Serienummer: 7c4880fb-fcb7-4e91-a742-e40e16321dfb*
*IP: 77.66.xxx.xxx*
*2026-02-26 13:54:01 UTC*

**Jesper Due Sørensen**
**EY Godkendt Revisionspartnerselskab CVR: 30700228**
**Partner**
*På vegne af: EY Godkendt Revisionspartnerselskab*
*Serienummer: a6d834d7-442d-428e-ade9-c250dca23ab3*
*IP: 5.103.xxx.xxx*
*2026-02-26 14:44:17 UTC*

**Jan Krarup Mortensen**
**EY Godkendt Revisionspartnerselskab CVR: 30700228**
**Statsaut. revisor**
*På vegne af: EY Godkendt Revisionspartnerselskab*
*Serienummer: 7ced7734-efa6-4690-a309-bc4d226937ad*
*IP: 37.96.xxx.xxx*
*2026-02-26 15:19:17 UTC*