

# CATALYSTONE SOLUTIONS

ISAE 3000 – INDEPENDENT AUDITOR’S ASSURANCE REPORT ON  
INTERNAL CONTROL RELATED TO INFORMATION SECURITY  
AND PRIVACY (GDPR)

Period: January 1<sup>st</sup> – December 31<sup>st</sup>, 2024

# Table of contents

SECTION 1 - BDO'S INDEPENDENT REPORT

SECTION 2 - MANAGEMENT STATEMENT

To: The Management of CatalystOne Solutions AS

## INDEPENDENT AUDITOR'S ASSURANCE REPORT ON INTERNAL CONTROL RELATED TO INFORMATION SECURITY AND PRIVACY (GDPR)

### Scope

We have been engaged to report on CatalystOne Solutions AS' description and compliance, in Section 3, of the internal control system with respect to processing personal data, with regards to EU's General Data Protection Regulation (GDPR) and the "law on the processing of personal data" (Personal Data Act), in addition to the information security policies put in place to secure the personal data's confidentiality, integrity and availability, throughout the period from January 1<sup>st</sup>, 2024 to December 31<sup>st</sup>, 2024, and on the design and functions of controls related to the control objectives stated in the description.

### CatalystOne Solutions' Responsibilities

CatalystOne Solutions is responsible for: preparing the description and accompanying statement in Section 3, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives; 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 *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

BDO AS applies International Standard on Quality Management 1 and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

### Auditor's Responsibilities

Our responsibility is to express an opinion on CatalystOne Solutions' description and on the design and operation 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 Engagement 3000, *Assurance engagements other than audit or reviews*

*of historical financial information*, issued by the International Auditing and Assurance Standards Board.

This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively in all material respects.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its systems, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment 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 CatalystOne Solutions AS and described in Section 3.

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

#### **Limitations of controls at CatalystOne Solutions**

CatalystOne Solutions' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the internal control system that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organization may not prevent or detect all errors or omissions in processing of personal data.

#### **Opinion**

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in Section 3. In our opinion, in all material respects:

- a) The description fairly presents the system and the controls of relevance to the description and compliance of the internal control system with respect to processing of personal data with regards to GDPR and the Personal Data Act, and the information security policies put in place to secure the personal data's confidentiality, integrity and availability throughout the period from January 1<sup>st</sup>, 2024 to December 31<sup>st</sup>, 2024; and
- b) The controls related to the control objectives stated in the description were suitably designed throughout the period from January 1<sup>st</sup>, 2024 to December 31<sup>st</sup>, 2024; 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 January 1<sup>st</sup>, 2024 to December 31<sup>st</sup>, 2024.



### **Description of test 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 controls included in Section 3 are exclusively intended for data controllers who have used CatalystOne Solutions for processing of personal data, who have a sufficient understanding to consider it, along with other information including information about controls operated by customers themselves, when assessing the requirements of EU's GDPR, Personal Data Act, and the data and information security when processing personal data.

Oslo, January 2025

**BDO AS**

***DIGITALLY SIGNED***

Terje Tvedt

State Authorized Public Accountant

# PENNEO

Signaturene i dette dokumentet er juridisk bindende. Dokument signert med "Penneo™ - sikker digital signatur". De signerende parter sin identitet er registrert, og er listet nedenfor.

"Med min signatur bekrefter jeg alle datoer og innholdet i dette dokument."

**Tvedt, Terje**

**Partner**

På vegne av: BDO

Serienummer: no\_bankid:9578-5992-4-3003934

IP: 188.95.xxx.xxx

2025-01-13 16:55:07 UTC



Dette dokumentet er signert digitalt via **Penneo.com**. De signerte dataene er validert ved hjelp av den matematiske hashverdien av det originale dokumentet. All kryptografisk bevisføring er innebygd i denne PDF-en for fremtidig validering.

Dette dokumentet er forseglest med et kvalifisert elektronisk segl ved bruk av et sertifikat og et tidsstempel fra en kvalifisert tillitstjenesteleverandør.

#### Slik kan du bekrefte at dokumentet er originalt

Når du åpner dokumentet i Adobe Reader, kan du se at det er sertifisert av **Penneo A/S**. Dette beviser at innholdet i dokumentet ikke har blitt endret siden tidspunktet for signeringen. Bevis for de individuelle signatørens digitale signaturer er vedlagt dokumentet.

Du kan bekrefte de kryptografiske bevisene ved hjelp av Penneos validator, <https://penneo.com/validator>, eller andre valideringsverktøy for digitale signaturer.

# Management Statement

# MANAGEMENT STATEMENT

CatalystOne Solutions AS (hereby referred to as CatalystOne Solutions) processes personal information on behalf of our customers. The purpose of processing information on behalf of the customer is to provide IT systems for the handling of HR information for the customer. All data collected and entered in the IT systems is owned and controlled by the customer. The customers of CatalystOne Solutions is the Controller in accordance with EU's General Data Protection Regulation on "the protection of individuals with regards to processing of personal data and on the free movement of such data" (hereby referred to as "GDPR") and the "law on the processing of personal data" (hereby referred to as "Personal Data Act").

The accompanying description has been prepared for the use of customers who have used CatalystOne Solutions' IT systems, who have a sufficient understanding to consider the description along with other information, including information about the control environment and system, that the controllers themselves have performed when evaluating if the criteria of the GDPR and Personal Data Act are complied with, and the security policies put in place to secure the personal data.

CatalystOne Solutions confirms that:

- a) The accompanying description in Section 3 fairly presents how CatalystOne Solutions has processed personal data for the Controller covered by the GDPR and Personal Data Act throughout the period from January 1<sup>st</sup>, 2024 to December 31<sup>st</sup>, 2024. The criteria used in making this statement were that the accompanying description:
  - i) Presents how CatalystOne Solutions' control environment was designed and implemented, including explaining:
    - The types of services provided, including the type of processed personal data;
    - The processes in both IT and manual systems that are used to initiate, register, process and, if necessary, delete and restrict personal data;
    - The processes used to ensure that data processing has been carried out under contract, instruction or agreement with the Controller;
    - The processes that ensure that the persons authorized to process data have committed themselves to confidentiality or are subject to appropriate statutory confidentiality;
    - The processes that, at the end of data processing, ensure that after the Controller's choice, deletion or return of all personal data to the Controller, unless law or regulation prescribes the retention of personal data;
    - The processes that in case of personal data breach support the Controller's ability to report to the supervisory authority and notify the registered persons;
    - The processes that ensure appropriate technical and organizational measures for the processing of personal data considering the risks posed by processing, by accidental or illegal destruction, loss, alteration, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed;
    - Controls regarding the design of the IT system that should be implemented by the Controller and which are necessary to achieve the control objectives specified in the description, are identified in the description;
  - How the internal control was designed and implemented to ensure and secure the confidentiality, integrity and availability of the personal data and information being processed, including:
    - The information transfer procedures, security controls, and access management when receiving and retrieving personal customer data;



- Processing instructions provided by the customers, controls to ensure information security with subcontractors, processing controls, and access management when processing personal customer data;
  - Procedures to restore accessibility and information transfer routines when processing output from the personal customer data;
  - Automatic procedures when deleting customer data.; and
- 
- Other aspects of our control environment, risk assessment process, information system (including the associated business processes) and communication, control activities and monitoring controls that have been relevant to the processing of personal data.
- 
- ii) Contains relevant information about changes for processing personal data throughout the period from January 1<sup>st</sup>, 2024, to December 31<sup>st</sup>, 2024; and
  - iii) Does not omit or distort information relevant to the scope of the customer for processing personal data taking into consideration that the description has been prepared to meet the general needs of a wide range of Controllers.
- 
- b) The controls associated with the control objectives listed in the accompanying description were appropriately designed and operating effectively throughout the period from January 1<sup>st</sup>, 2024, to December 31<sup>st</sup>, 2024. The criteria used to give this assurance were that:
    - i) The risks posed by the achievement of the control objectives set out in the description were identified;
    - ii) The identified controls would, if carried out as described, provide a high level of assurance that the risk involved did not prevent the achievement of the specified control objectives; and
    - iii) The controls were used consistently as designed, including that manual controls were performed by individuals who have the appropriate competence and authority throughout the period from January 1<sup>st</sup>, 2024 to December 31<sup>st</sup>, 2024.
- 
- c) Appropriate technical and organizational measures have been established and maintained to comply with the agreements with the Controller, good data processing practices, relevant data processing requirements under the GDPR and Personal Data Act, and information security policies securing confidentiality, integrity and availability of personal data.

Oslo, January 2025

***DIGITALLY SIGNED***

Avtar Singh Jasser  
CEO, CatalystOne Solutions AS

# PENNEO

Signaturene i dette dokumentet er juridisk bindende. Dokument signert med "Penneo™ - sikker digital signatur". De signerende parter sin identitet er registrert, og er listet nedenfor.

"Med min signatur bekrefter jeg alle datoer og innholdet i dette dokument."

**Jasser, Avtar Singh**

CEO

På vegne av: CatalystOne Solutions AS

Serienummer: no\_bankid:9578-5993-4-3269263

IP: 195.159.xxx.xxx

2025-01-13 16:43:52 UTC



Dette dokumentet er signert digitalt via **Penneo.com**. De signerte dataene er validert ved hjelp av den matematiske hashverdien av det originale dokumentet. All kryptografisk bevisføring er innebygd i denne PDF-en for fremtidig validering.

Dette dokumentet er forseglet med et kvalifisert elektronisk segl ved bruk av et sertifikat og et tidsstempel fra en kvalifisert tillitstjenesteleverandør.

#### Slik kan du bekrefte at dokumentet er originalt

Når du åpner dokumentet i Adobe Reader, kan du se at det er sertifisert av **Penneo A/S**. Dette beviser at innholdet i dokumentet ikke har blitt endret siden tidspunktet for signeringen. Bevis for de individuelle signatørens digitale signaturer er vedlagt dokumentet.

Du kan bekrefte de kryptografiske bevisene ved hjelp av Penneos validator, <https://penneo.com/validator>, eller andre valideringsverktøy for digitale signaturer.