ROESGAARD

NÅR OVERBLIK SKABER VÆRDI

Enreach Campaigns A/S

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with customers related to Outbound by Enreach, throughout the period from 1 September 2024 to 31 August 2025

Contents

Section 1: Enreach Campaigns A/S' statement 3

Section 2: Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with customers related to Outbound by Enreach throughout the period from 1 September 2024 to 31 August 2025 5

Section 3: Enreach Campaigns A/S' description of processing activity for the supply of Oubound by Enreach 8

Section 4: Control objectives, controls, tests, and results hereof 20

Section 1: Enreach Campaigns A/S' statement

The accompanying description has been prepared for data controllers, who has signed a data processing agreement with Enreach Campaigns A/S, and who has a sufficient understanding to consider the description along with other information, including information about controls operated by 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.

Enreach Campaigns A/S uses the following sub-processors: Global Connect A/S, Digital Reality and Amazon Web Services. This statement does not include control objectives and related controls at Enreach Campaigns A/S' sub-processors. Certain control objectives in the description can only be achieved, if the sub-processor's controls, assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities performed by sub-processors.

Some of the control areas, stated in Enreach Campaigns A/S' description in Section 3 of Outbound by Enreach, can only be achieved if the complementary controls with the data controllers are suitably designed and operationally effective with Enreach Campaigns A/S' controls. This assurance report does not include the appropriateness of the design and operational effectiveness of these complementary controls.

Enreach Campaigns A/S confirms that:

a) The accompanying description, Section 3, fairly presents how Enreach Campaigns A/S has processed personal data for data controllers subject to the Regulation throughout the period from 1 September 2024 to 31 August 2025. The criteria used in making this statement were that the accompanying description:

(i) Presents how Enreach Campaigns A/S' processes and controls were designed and implemented, including: // This includes the processes and controls described

- The types of services provided, including the type of personal data processed
- 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
- The procedures used to ensure that data processing has taken place in accordance with contract, instructions, or agreement with the data controller
- 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
- 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
- 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
- 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

- Controls that we, in reference to the scope of Enreach Campaigns A/S, 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
- 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 about changes in the data processor's Outbound by Enreach in the processing of personal data throughout the period from 1 September 2024 to 31 August 2025;

(iii) Does not omit or distort information relevant to the scope of Outbound by Enreach 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 Outbound by Enreach 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, in our view, suitably designed and operated effectively throughout the period from 1 September 2024 to 31 August 2025 and if relevant controls with sub-processors were operationally effective and data controller has performed the complementary controls, assumed in the design of Enreach Campaigns A/S' controls throughout the period from 1 September 2024 to 31 August 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 September 2024 to 31 August 2025.

c) Appropriate technical and organisational 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.

Hvidovre, 9. Januar 2026
Enreach Campaigns A/S

Casper Langhoff
CEO

Section 2: Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with customers related to Outbound by Enreach throughout the period from 1 September 2024 to 31 August 2025

To: Enreach Campaigns A/S and their customers

Scope

We were engaged to provide assurance about a) Enreach Campaigns A/S' description in Section 3 of Outbound by Enreach in accordance with the data processing agreement with customers throughout the period from 1 September 2024 to 31 August 2025 and about b+c) the design and operational effectiveness of controls related to the control objectives stated in the description. Enreach Campaigns A/S uses the following sub-processors Global Connect A/S, Digital Reality and Amazon Web Services. This statement does not include control objectives and related controls at Enreach Campaigns A/S' subprocessors. Certain control objectives in the description can only be achieved if the subprocessor's controls, assumed in the design of our controls, are appropriately designed, and operating effectively. The description does not include control activities performed by subprocessor. Some of the control objectives stated in Enreach Campaigns A/S' description in Section 3 of Outbound by Enreach, can only be achieved if the complementary controls with the data controllers have been appropriately designed and operating effectively with the controls with Enreach Campaigns A/S. The report does not include the appropriateness of the design and operational effectiveness of these complementary controls.

Enreach Campaigns A/S' responsibilities

Enreach Campaigns A/S is responsible for: preparing the description and the accompanying statement, 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; and for the design and implementation of operationally effective controls, to achieve the stated control objectives.

Roesgaard's 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 behavior and ethical requirements applicable to Denmark. Roesgaard is subject to the International Standard on Quality Control (ISQM1) and accordingly uses and 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 Enreach Campaigns A/S' description and on the design and operational 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 regulations, 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 a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of Outbound by Enreach 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 appropriately 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 appropriateness of the objectives stated therein, and the appropriateness 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 processor

Enreach Campaigns A/S' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Outbound by Enreach 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 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 the *Management's statement* Section 1. In our opinion, in all material respects:

a) The description fairly presents Outbound by Enreach as designed and implemented throughout the period from 1 September 2024 to 31 August 2025;

b) The controls related to the control objectives stated in the description were appropriately designed throughout the period from 1 September 2024 to 31 August 2025; to obtain reasonable assurance that the control objectives stated in the description would be obtained if controls with subprocessor were operating effectively and if data controller has designed and implemented the

complementary controls, assumed in the design of Enreach Campaigns A/S' controls throughout the period from 1 September 2024 to 31 August 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 September 2024 to 31 August 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 Enreach Campaigns A/S' Outbound by Enreach 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.

Horsens, 9. januar 2026

Roesgaard
Godkendt Revisionspartnerselskab

Michael Mortensen
Partner, Statsautoriseret revisor

Section 3: Enreach Campaigns A/S' description of processing activity for the supply of Oubound by Enreach

Introduction

The purpose of this description is to supply information to Enreach Campaigns' customers and their stakeholders (including auditors) regarding the requirements and contents of the EU General Data Protection Regulation ("GDPR"), as described by the framework of the International Standard for Assurance Engagements ISAE 3000.

Additionally, the purpose of this description is to provide specific information on matters regarding the security of processing, technical and organisational measures, responsibility between data controllers (our customers) and processors (Enreach Campaigns), and how the solution Outbound by Enreach by means of functionality for e.g. supporting the rights of the data subjects, support our customers (the data controllers) in relation to complying with GDPR as regards their activities in Outbound by Enreach. Thus, the description is applicable for our delivery of the product and service Outbound by Enreach to our customers.

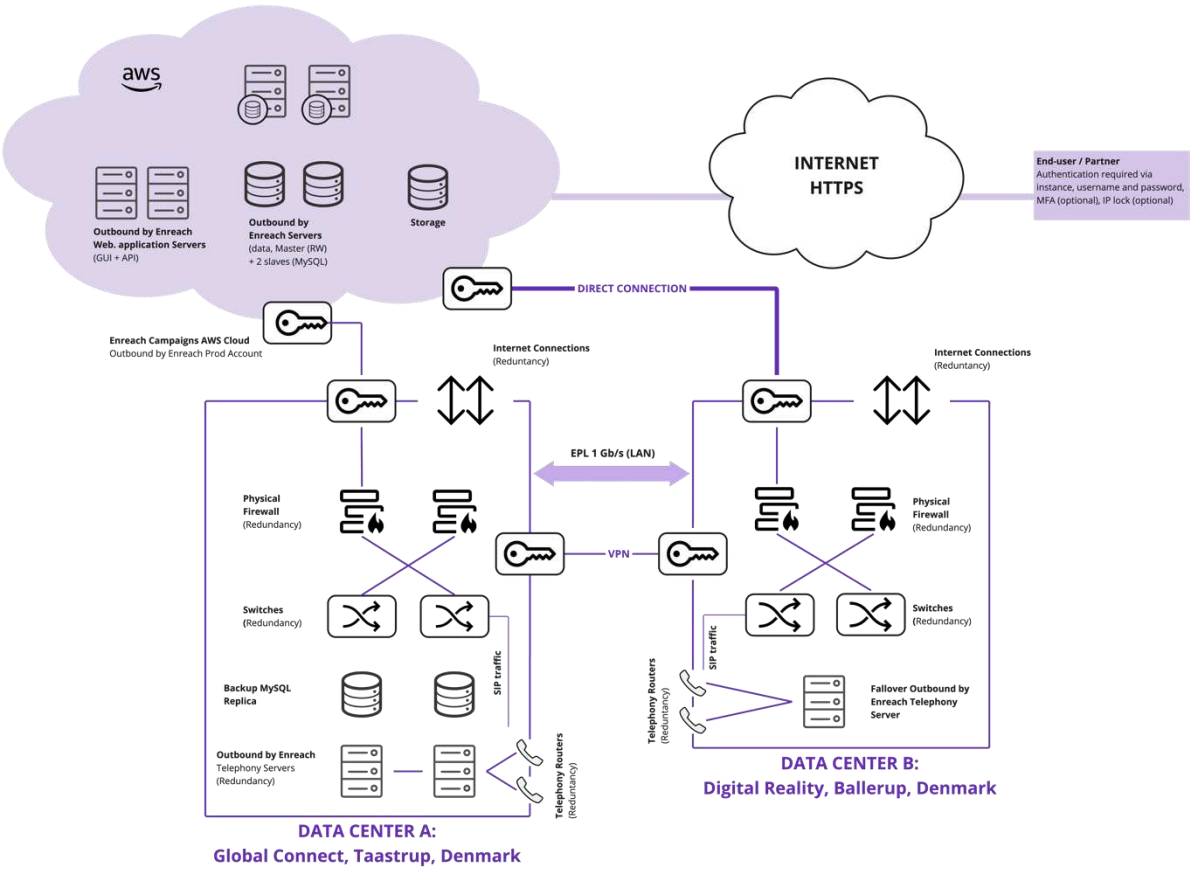
The description concerns the matters related to Outbound by Enreach that cover the majority of our customers and are based on our standard delivery. Individual customer relations are not included in this description.

Enreach Campaigns and our software Outbound by Enreach

Enreach Campaigns is a Danish IT company based in Hvidovre. We develop, host, and supply software in the form of a SaaS solution to contact centres. One of our core products is supplying the software Outbound by Enreach (here-after just named "Outbound"), which is supplied as a SaaS-solution, which means it is hosted in our own data centres and is based on a flexible and scalable subscription-based model.

Technical setup and placement

Outbound is a web application based on .NET (the primary language is C#) and with a frontend based on e.g. JavaScript, Angular and REACT. The database technology is MySQL, and hosting is via the Danish data centres GlobalConnect (Taastrup) and Digital Reality (Ballerup) as well as AWS' (Amazon Web Services). Frankfurt and Dublin locations, and Enreach's European based data centres. The only AWS locations we have chosen services in, and where data thereby is located in, are AWS' Dublin site in Ireland and AWS' site in Frankfurt, and thereby no data in Outbound leaves the EU. Telephony-wise, calling is operated by physical Linux servers with Freeswitch as a teleoperating system on top. Our infrastructure and architecture are designed in such a way that there is redundant failover equipment for everything from firewalls and switches to database and web servers. Most of the equipment is also placed in both data centres, which means that one location can resume operations, if another location is impacted by reduced access or other problematic circumstances, internal as well as external.



Organisation and responsibility
Enreach Campaigns employs 23 persons in Denmark, Sweden, Ukraine, the UK, and Finland. About half the employees are placed in Denmark and have their daily workplace at the office in Hvidovre.

The management consists of an ultimately responsible Managing Director, and his direct report are Finance Manager (UK), Head of Tech (DK), Head of Growth (UK), and Head of Customer Relations (DK).

The Tech department, led by the Head of Tech, consists primarily of developers in a “DevOps” constellation, where two persons are dedicated to operations, optimising servers and infrastructure, monitoring and handling operational issues, but where all have operations as their first priority in case of technical issues on the platform.

The developers are organised in frontend and backend expertise, with a chief architect who makes the general decisions on language, technology, and new frameworks on the basis of a thorough analysis and in cooperation with the Head of Tech. In addition, a network administrator is responsible for network and telephony, whereas a project manager and tester have a close cooperation with Enreach Campaigns’ other departments.

Management has the overall responsibility for IT security and that the company’s general IT security policy is observed.

Next to the daily organisation based on function, a security organisation has been organised with an Information Security Committee comprising key employees from various parts of Enreach Campaigns, including management, and an information security coordinator who has the daily, operational responsibility for a number of tasks defined in Enreach Campaigns' information security code of practice. The information security coordinator is additionally responsible for all employees being aware of the information security manual, including rules and procedures, helps them to access and understand it, and acting on and observing the rules. In conclusion, the responsibility for a variety of matters related to the business systems that support the daily work with supplying the product and service Outbound is delegated to the system owners.

Risk management in Enreach Campaigns A/S
Risk management in Enreach Campaigns A/S is done for all areas connected with delivering the product and service Outbound, and which thereby may have financial consequences for our customers. Risk analysis, assessment, and management are based on ISO 27005, and are based on impact analyses and vulnerability analyses at service level. Service is understood as business systems supporting the delivery of Outbound as well as Outbound in itself as a customer system.

The business in Enreach Campaigns answers the questions in the impact analysis, while the IT department in Enreach Campaigns performs the vulnerability analysis.

Risk analyses are conducted as consequence and vulnerability analyses at least annually, after which the collected security overview is brought up for the information security committee and finally Enreach Campaigns' management, for the definition of further actions.

Generally, on our control objectives, including rules and procedures as well as implemented controls
The most important thing in the supply of the product and service Outbound is a stable and secure platform. It is a declared and management embedded promise that we would rather spend twice the time on solving a development task or another technical task than what was strictly necessary to solve the task, in order to ensure security and stability when we release updates to our customers.

To ensure that the supply chain can function, and that Enreach Campaigns at the same time can function as a competitive business, including achieving scalability over time, working procedures and processes connected with the supply of the product and service, Outbound are based on our information security code of practice, on top of which are defined procedures and controls with associated contingency plans etc.

The framework for the information security code of practice is ISO 27001, and the code of practice is classified according to the following control areas:

- Information security management and security policy
- Organisation of information security
- Human resource security
- Access control

- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development, and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

In addition, we have selected a number of procedures and policies within the framework of data security and GDPR. As a processor we have furthermore ensured that we have data processing agreements with all our cusomers on Outbound who in this constellation are data controllers.

GDPR and Enreach Campaigns' role and responsibility as a processor
GDPR is for everybody – but it is essential to understand how the specific parts of GDPR find use for each player depending on the type of organisation in question, and how the organisation is subject to activities connected with the processing of data.

As the provider of the software and solution Outbound, Enreach Campaigns is the processor for all our customers. This means that we in our software Outbound are hosting data that belongs to our customers as data controllers, and that we via our software provide a selection of tools and functionality that our customers – the data controllers – can use for working with the data. We only act on instruction from our customers and the framework for these instructions is defined in the contract between the customer and Enreach Campaigns as well as the associated processor agreement.

The following sections examine these measures and aspects in detail with a focus on Enreach Campaigns' role as a processor, i.e. measures that concern our processing of the data controllers' data, and how our software Outbound is designed to support our customers as data controllers when it comes to the requirements that GDPR poses to data controllers.

Principles relating to processing of personal data
Outbound is a generic and flexible platform that enables the input and entering of all sorts of data in principle. Campaign templates, fields (with associated attributes such as type of data, field validation, etc.) are defined, created, and maintained by the customer itself that fully decides and is responsible for what data is input in, stored in, processed in, read out, and deleted from Outbound.

Enreach Campaigns as a supplier neither accesses nor processes these data, unless we receive an explicit instruction from the data controlling customer for aiding with e.g. inputting data or rectifying/changing data in connection with the customer's campaign activities.

There is a data processing agreement between Enreach Campaigns and all customers. The contents and principles for this are specified in later sections.

Through procedures and training Enreach Campaigns has ensured that the classification of customer data and the associated processing principles are known by all employees.

Lawfulness of processing
If Enreach Campaigns receives instructions from the customer that are assessed to be contrary to current legislation or general sound principles for data processing, Enreach Campaigns will without undue delay bring this to the customer's attention.

Enreach Campaigns does not under any circumstances exchange or disclose the customer's data to third parties. An exception to this is situations where national special legislation requires that Enreach Campaigns provides information, e.g. if Danish authorities request data on certain phone calls as part of an investigation. In such cases the only personally identifiable data disclosed will be a phone number – no other personal data will be provided.

We have defined controls ensuring that customer data is not accessed by employees in other situations than helping the customer with support, or if separate instructions have been received from the customer.

Processing of various categories of personal data
We have classified all data belonging to our customers as data controllers as "customer data".

We have a processing agreement with all our customers. When this is based on Enreach Campaigns' processing agreement template, we have asked the customer to account for what types of personal data (categorised according to Article 6, 9, 10, respectively 87) the customer intends to input and enter into Outbound.

Rights of the data subject
Outbound registers all changes to data for a lead processed in our software, as well as all interactions with the lead in question.

As data controllers our customers can retrieve all leads input into and processed in Outbound and see a full list of interactions with each lead.

As data controllers our customers can retrieve all leads input into and processed in Outbound and see a full list of all data present on each lead.

Thereby all processing activities are explicitly registered and are available to the customer directly in Outbound's user interface.

As data controllers our customers can retrieve individual leads, block them for future contact, and/or delete all data present on each lead.

As data controllers our customers can retrieve individual leads and edit/rectify information on each lead.

As data controllers our customers can export the above-mentioned data, such that data can be transferred to a data subject; deleted from Outbound, and that the data subject with its data can be moved to another system or service.

Thereby Outbound supports our customers as data controllers when it comes to complying with the rights of the data subjects and as a starting point handling these efficiently and without undue delay.

General obligations as processor
We have procedures that ensure that we comply with our obligations as a processor and to the widest extent possible support our customers as data controllers in relation to the requirements that GDPR poses to them.

Our functions for supporting the rights of the data subjects, cf. the previous section, are collected on a few different pages in Outbound that through module and rights management at the customer itself ensures our customers' possibility of allocating functional rights to using the functions according to a work-related need at the customer.

If Enreach Campaigns should receive an application directly from a data subject, instead of via the customer, Enreach Campaigns will within the framework of the legislation request further information from the data subject, and without undue delay forward the application or request to our customer. This is communicated to and trained with our employees.

We have ensured processing agreements with subprocessors, including hosting and housing partners.

We have ensured that the requirements imposed by data controllers on us through the contract and the processing agreement correspondingly are imposed on sub-suppliers and sub data processors.

Through training and campaigns, we ensure awareness of significant areas within information security, data protection, as well as (but not limited to) GDPR.

We have procedures for data protection being part of the considerations and choices regarding design when Outbound is changed and improved.

Acting according to instruction from our data controlling customers also include how long data is stored in Outbound. Data is here understood as written data (numerical values, text strings and other entries – what traditionally is understood as data) and multimedia data (audio files from conversations that our customers have decided to record via Outbound).

Instructions are given to Enreach Campaigns as processor through settings that the customer configures in Outbound.

Security of processing, notification, and communication
We have established adequate technical and organisational measures, which are detailed in a later main section.

We have chosen ISO 27001 to be the information security framework that our information security code of conduct, procedures, and controls are based on.

We have procedures for managing information security incidents, including data breaches, as well as information security incidents.

Notification to relevant authorities, in cases where this is necessary, as well as notification to our customers as data controllers in case incidents or events concern these or might do so, is done within set time limits that are defined in the processor agreements.

Data protection impact assessment
We have procedures for conducting data protection impact assessments (DPIA) in connection with the conduction of projects and development of Outbound as software.

Our hosting and housing partners, which we have sub data processing agreements with, only have data stored in the EU, cf. previous section. Data in Outbound is thus never transferred to third countries unless the customer decides to do this outside of the engagement with Enreach Campaigns.

Technical and organisational measures
In this section we will elaborate on a number of matters regarding Enreach Campaigns' technical and organisational measures regarding the supply and operation of the software and solution Outbound

Human resource security
We have defined a number of procedures that ensure security prior to, during, and, if relevant, after employment.

Procedures concerning processes before a potential employment ensure that potential employees are screened and that relevant matters are checked within the framework of current legislation.

All employees must adhere to a number of terms regarding confidentiality about own, Enreach Campaigns', and customers' matters. This is described in each employee's employment contract.
During employment it is ensured between the employee, the immediate manager, and the information security coordinator that the employee is kept up to date regarding and comply with aspects regarding information security.

We have procedures that ensure that employees at the termination of employment cannot cause damage to Enreach Campaigns, or the system Outbound by means of immediately removing rights to business systems and check this.

Access management
We have a string of procedures that ensure that access control and the allocation of rights occur in compliance with the established security level.

Only employees with a work-related need for having access to systems and data are granted access to the concerned business systems and associated data.

The heads of department are responsible for access rights being granted on the basis of a work-related need and in consideration of regulatory and contractual obligations.

We control that this occurs on an ongoing basis, and that all access corresponds to the work-related needs in each function and for each employee.

We have defined a string of requirements for the protection of all devices (PCs, mobile phones, tablets) as well as passwords in all business systems. Employees are trained and checked within these areas.

We have a number of procedures that ensure that only a group of privileged employees has access to system administrator tools, central servers (e.g. domain controller), source code etc.

Production servers and other servers containing production data and customer data are only present in Enreach Campaigns' data centres and not at any office locations. Only specially trusted employees with a work-related need have access to the data centres. These accesses are assessed and inspected regularly via onboarding, offboarding procedures and ad hoc controls.

Cryptography
We have procedures for the use of cryptography, including the generation and management of encryption keys and certificates.

This means, i.a., that Outbound must have a valid SSL certificate, which Enreach Campaigns verifies, such that data exchange only occurs in a secure and encrypted manner (through HTTPS). SSL-certificates are managed solely by the IT department, where the application architect and network administrator are responsible for SSL certificates. No certificates may be acquired or issued bypassing these.

This requirement concerns access to Outbound through the user interface and through API alike.

Physical and environmental security
Servers are only placed in data centres provided by suppliers who have been issued, and annually can show, assurance reports at the level of ISAE 3402.

Enreach Campaigns' office premises are subject to a number of procedures that secure the office as well as material and units stored at the office, regardless of servers only being placed in data centres.

This entails, i.a., procedures aimed at employees describing security measures for offices, common areas, and similar areas.

Operations security
Operating procedures and monitoring
We have operating procedures for the IT department's most significant duties, and these procedures are subject to versioning and change management.

We have defined the responsibility for ensuring that an assessment of the capacity requirements for critical IT systems is performed regularly.

The IT department, led by the Head of Tech, consists primarily of developers in a "DevOps" constellation, where two persons are dedicated to operations, optimising servers and infrastructure, monitoring and handling operational issues, but where all have operations as the first priority in case of technical issues on the platform or information security issues.

All instances of Outbound are monitored by means of monitoring tools.

Critical levels and values are defined for all these monitoring areas. Alarms must trigger when these values are reached and must be sent to key employees either via email (for less critical alerts) or SMS (critical alerts).

Development of Outbound, management, and quality assurance
The development of Outbound, including release of changes, occurs according to Enreach Campaigns' formalised and embedded development model.

Development occurs in development environments where code is branched from the main branch/"default". These development branches are connected with the staging database, where test data is found. Test data and production data are thus completely segregated, and customers' data must not be copied from master to staging without approval from the Head of Tech. If this permission is granted, it can and will only comprise configuration data in order to test and develop up against true, complex data in order to ensure the quality of the development, but it must and can never comprise data on the customer's prospects, employees or similar.

Function testing takes place in development branches (also called feature branches), after which code is tested and merged to pre-production branches, from which code is tested again prior to finally deployed for production.

Logging
We have procedures concerning the scope, processing, protection, and check of logging on various system types.

All logins and significant user actions in Outbound are monitored and logged. The logging of significant user actions concerns i.a. data export, such that customer administators have an overview over which users that access and export data.

All changes to data are registered. All significant changes to configurations are registered. These registrations are also available for customer administrators through visible logs in the user interface. The logging level also comprises employees at Enreach Campaigns, whereby it is checked that these do not access customer data without a work-related need for this.

Communications security
We have procedures for network management and monitoring, including maintenance of network and network equipment.

Traffic on all connections and interfaces are monitored in relation to data volume over periods of time. Alarms have been set up that are triggered and sent to technical personnel in case of abnormalities (traffic spikes, significant delays between master databases and slave databases, and much else). Regarding tele connections, the amount of provider channels, the amount of server channels (Freeswitch channels), and number of ongoing calls, amongst other things, are monitored, and max values for periods of time are logged.

Exchange of information solely occurs by means of secure connections. If this occurs via the public Internet, data is encrypted (in principle by means of HTTPS). via LAN.

Supplier relationships
In all cooperation agreements with suppliers, we have defined security requirements and minimum requirements for the services provided to us by the supplier.

We have ensured that the matters we base our agreement on regarding the use of the product and service Outbound in relation to customers, are in accordance with our requirements to our suppliers.

We regularly, and at least annually, review the assurance reports for the entered agreements.

Information security incident and event management

The information security committee has defined procedures for information security incidents and events, which are embedded in Enreach Campaigns and which the management is responsible for being observed.

We define information security incidents as:

- The detection of successful external and unwanted intrusion in systems
- Finding customer data (hosted in the master database for Outbound) online, where there is an obvious or strong suspicion that the publication of data has not occurred with the customer's approval and intent

- Finding data on current or former employees in Enreach Campaigns online, where publication of data has occurred without Enreach Campaigns' involvement or intent
- Finding other confidential business data online (according to the same directions) defined as customer contracts, revenue, or information which is classified as secret according to further definition by the information security committee

We define information security events as:

- Events that, if they had not been discovered, could have led to security incidents
- Situations where unintended data or information by accident (due to human error) has been sent to other recipients than the intended, and that it is assessed that this may entail damage or serious consequences for Enreach Campaigns

Procedures have been defined for both, which describe for employees and managers how they should act in case of incidents and events, including (but not limited to) collecting evidence and contact with authorities, if necessary.

Record of processing activities
We have a list of record of processing activities for Enreach. This record of processing activities is based on our agreements with data controllers.

Complementary controls

Regarding our customers, Enreach Campaigns is responsible for delivering the services and the operations described in the contract concerning Outbound between the customer and Enreach Campaigns.

Matters not comprised by the contract are the customer's own responsibility.

Creation of users, protection of user information, and secure login procedures are the responsibility of the customer. The customer can by writing to Enreach Campaigns request the establishment of an IP lock on the customer's Outbound account, whereby login only will be possible from explicitly defined whitelisted IP addresses. Enreach Campaigns recommends our customers to do this to the extent it is possible for the customer, in order to protect the customer's data and activities in Outbound.

Regarding data uploaded to Outbound by the customer, it is a significant division of responsibility that the customer is the data controller, and Enreach Campaigns is the processor. Thus, Enreach Campaigns only acts according to instructions from the customer. In the contract or in the processing agreement that the customer provides En- reach Campaigns the customer gives an indication to Enreach Campaigns of what types/categories of data that the customer intends to upload to and process in Outbound. A processing agreement must be established between Enreach Campaigns and the customer.

It is the customer's responsibility to have defined and embedded a procedure at the customer that ensures compliance with GDPR by i.a. complying with the requirements of response time regarding enquiries from private individuals/data subjects. Enreach Campaigns provides functions through the tool Outbound, but

cannot be held responsible for the customer's definition, embedding, and observation of procedures that are to ensure the customer's compliance.

Changes in the audit period
No significant changes in the period.

Section 4: Control objectives, controls, tests, and results hereof

We conducted our engagement in accordance with ISAE 3000, assurance engagements other than audits or review of historical financial information. Our test of the functionality has included the control objectives and attached controls, selected by management and which are stated in the control objectives A-I below. Our test has included the controls we find necessary to establish reasonable assurance for compliance with the articles stated throughout the period from 1 September 2024 to 31 August 2025.

Our statement does not apply to controls performed at Enreach Campaigns A/S' sub-processors.

Further, controls performed at the data controller are not included in this statement.

We performed our test of controls at Enreach Campaigns A/S by the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at Enreach Campaigns A/S. The interviews have included questions about how controls are performed.
Observation	Observing how controls are performed.
Inspection	Review and evaluation of policies, procedures and documentation concerning the performance of controls. This includes reading and assessment of reports and documents in order to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented. Further, it is assessed whether controls are monitored and controlled adequately and with suitable intervals. The effectiveness of the controls during the audit period is assessed by sample testing.
Re-performance	Re-performance of controls to verify that the control is working as assumed.

Control objective A - Instructions regarding processing of personal data **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.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
A1	Written procedures exist 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 – as to whether the procedures should be updated.	We have inspected that formalised procedures exist to ensure that personal data are only processed according to instructions. We have inspected that procedures are up to date.	No deviations noted.
A2	The data processor only processes personal data stated in the instructions from the data controller.	We have inquired about how management ensures that personal data are only processed according to instructions. We have inspected that a sample of personal data processing operations are conducted consistently with instructions.	No deviations noted.

A3	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.	We have inspected that there are procedures for notifying the data controller in cases where the processing of personal data is deemed to be in violation of the law. We have inquired into whether the data processor has received instructions that, in the opinion of the data processor, are in conflict with the General Data Protection Regulation or data protection provisions in other EU law or the national law of the Member States.	We have been informed that the data processor has not received instructions that, in the opinion of the data processor, are in conflict with the General Data Protection Regulation or data protection provisions in other EU or Member States' national law, wherefore we have not tested the effectiveness of relevant procedures. No deviations noted.
Control objective B - Technical measures **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
B1	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. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist to ensure establishment of the safeguards agreed. We have inspected that procedures are up to date. We have, by sample test, inspected documentation that the agreed security measures have been established.	No deviations noted.
B2	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.	We have inspected that the risk assessment carried out is up to date and includes the current processing of personal data.	No deviations noted.

B3	For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.	We have inspected that the systems and databases used in the processing of personal data, protection against malware have been implemented.	No deviations noted.
B4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	We have inspected that there are defined requirements for the management and control of networks. We have walked through the process of monitoring and use of controls to protect the systems and data.	No deviations noted.
B5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	We have inspected technical documentation to show that there is separation of environments used in systems.	No deviations noted.

B6	Access to personal data is isolated to users with a work-related need for such access.	We have inspected that formalised procedures are in place for restricting users' access to personal data. We have inspected that new hires during the period have had their user access rights approved. We have, by sample, inspected that resigned users' access rights have been revoked. We have inspected that a review and evaluation of access rights is carried out during the period.	No deviations noted.
B7	For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.	We have inspected the procedure for monitoring use of resources and adjustments of capacity, to ensure future capacity Requirements. We have inspected that relevant platforms are included in the capacity requirement procedure.	No deviations noted.
B8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	We have inspected the policy for the use of encryption. We have inspected that transmission over the internet is done with a secure connection.	No deviations noted.

B9	Logging has been established in systems, databases, and networks. Log data are protected against manipulation and technical errors.	We have inspected procedures for logging of user activities. We have inspected that logging configurations contain user activities, exceptions, faults, and incidents. We have inspected procedures for securing log information. We have inspected that access to logging information is restricted.	No deviations noted.
B11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	We have inspected that penetration tests have been carried out during the period. We have inspected that antivirus software has been installed on the systems and databases used for the processing of personal data. We have inspected that systems are patched.	No deviations noted.
B12	Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches.	We have inspected the procedure for changes in information processing facilities and systems. We have inspected that the ongoing control of changes following the procedure has been carried out during the period.	No deviations noted.

B13	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 workrelated need.	We have inspected that formalised procedures for user registration and de-registration have been established. We have inspected that new hires during the period have had their user access rights approved. We have inspected that resigned users' access rights have been revoked. We have inspected the procedure for regular review and evaluation of access rights. We have inspected that a review and evaluation of access rights is carried out during the period	No deviations noted.
B14	Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication.	We have inspected the procedure for secure logon. We have inspected, that MFA has been established in connection with logon.	No deviations noted.
B15	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.	We have inspected the procedure for physical protection of facilities and perimeter security. We have inspected that access to locations with equipment is limited to employees who need the access.	No deviations noted.

Control objective C - Organisational measures **Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
C1	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 – as to whether the IT security policy should be updated.	We have inspected that an information security policy exists that management has considered and approved within the past year. We have inspected documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No deviations noted.
C2	Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.	We have inspected documentation for management's assessment that the information security policy generally complies with the requirements in the data processing agreements. We have, by sample, inspected that the requirements in the data processing agreements are covered by the information security policy's requirements.	No deviations noted.
C3	The employees of the data processor are screened as part of the employment process.	We have inspected the procedure for screening new employees. We have inquired about screening of new employees during the period. We have inspected documentation that new employees have been screened.	No deviations noted.

C4	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 inspected the procedure for onboarding new employees. We have inspected documentation that new employees sign a confidentiality agreement and have been informed about their roles and responsibilities in information security.	No deviations noted.
C5	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.	We have 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. We have, by sample, inspected that rights have been deactivated or terminated and that assets have been returned for employees resigned or dismissed during the assurance period.	No deviations noted.
C6	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.	We have inspected 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. We have, by sample, inspected that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality for employees resigned or dismissed during the assurance period.	No deviations noted.

C7	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 inspected that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data. We have inspected documentation that all employees who have either access to or process personal data have completed the awareness training provided.	No deviations noted.
C8	The processor has assessed the need for a DPO and has ensured that the DPO has the adequate professional competence to perform their tasks and are involved in relevant areas.	We have inspected the assessment of the need for a DPO and ensured that the company has assessed the need for a DPO during the period.	Enreach has chosen not to appoint a DPO. No deviations noted.
C9	The processor keeps a record of categories of processing activities for each data controller.	We have inspected the existence of records of processing activities.	No deviations noted.
Control objective D - Return and deletion of personal data **Procedures and controls are complied with to ensure that personal data are deleted or returned if arrangements are made with the data controller to this effect.**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
D1	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 – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller. We have inspected that the procedures are up to date.	No deviations noted.
D2	Specific requirements have been agreed with respect to the data processor's storage periods and deletion routines.	We have inspected that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines.	No deviations noted.

D3	Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been: • Returned to the data controller; and/or • Deleted if this is not in conflict with other legislation.	We have inspected that formalised procedures are in place for the processing of the data controller's data upon cessation of processing of personal data. We have, by sample test of terminated data processing activities during the reporting period, inspected that documentation exists confirming that the agreed deletion or return of data has been carried out.	No deviations noted.
Control objective E – Storage of personal data **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.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
E1	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 – as to whether the procedures should be updated.	We have inspected that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements. We have inspected that the procedures are up to date.	No deviations noted.
E2	Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.	We have inspected that the data processor has a complete and updated list of processing activities stating localities, countries, or regions. We have, by sample test, inspected 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 F – Use of subprocessors **Procedures and controls are complied with to ensure that only approved subprocessors 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.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
F1	Written procedures exist which include requirements for the data processor when using subprocessors, including requirements for sub-data processing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place for using subprocessors, including requirements for sub-data processing agreements and instructions. We have inspected that procedures are up to date.	No deviations noted.
F2	The data processor only uses subprocessors to process personal data that have been specifically or generally approved by the data controller.	We have inspected that the data processor has a complete and updated list of subprocessors used.	No deviations noted.
F3	When changing the generally approved subprocessors 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 subprocessors used, this has been approved by the data controller.	We have inspected that there are formalised procedures for notifying the data controller of changes in the use of subprocessors. We have inquired into whether there have been any changes to subprocessors during the period.	We have been informed that there have been no changes in the use of subprocessors during the period. No deviations noted.

F4	The data processor has subjected the subprocessor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	We have inspected for existence of signed sub-data processing agreements with subprocessors used, which are stated on the data processor's list. We have, by sample test, inspected that sub-data processing agreements include the same requirements and obligations as are stipulated in the data processing agreements between the data controllers and the data processor.	No deviations noted.
F5	The data processor has a list of approved subprocessors.	We have inspected that the data processor has a complete and updated list of subprocessors used and approved. We have inspected that, as a minimum, the list includes the required details about each subprocessor.	No deviations noted.
F6	Based on an updated risk assessment of each subprocessor 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 subprocessor.	We have inspected that formalised procedures are in place for following up on processing activities at subprocessors and compliance with the sub-data processing agreements. We have inspected, that review and assessment of relevant audit reports on significant subservice organisations have been performed.	No deviations noted.

Control objective H – Rights of the data subjects **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.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
H1	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 – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects. We have inspected that procedures are up to date.	No deviations noted.
H2	The data processor has established procedures as 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.	We have inspected that the procedures in place for assisting the data controller include detailed procedures for: • Handing out data • Correcting data • Deleting data • Restricting the processing of personal data • Providing information about the processing of personal data to data subjects. We have asked whether the data processor has received any requests from the data controller in relation to the rights of the data subjects.	No deviations noted.

Control objective I – Managing personal data breaches **Procedures and controls are complied with to ensure that any personal data breaches are responded to in accordance with the data processing agreement entered into.**			
No.	Enreach Campaigns A/S' control activity	*Test performed by Roesgaard*	*Result of test*
I1	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 – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. We have inspected that procedures are up to date.	No deviations noted.
I2	The data processor has established controls for identification of possible personal data breaches.	We have inspected that the data processor provides awareness training to the employees in identifying any personal data breaches. We have inspected documentation that all employees who have either access to or process personal data have completed the awareness training provided.	No deviations noted.
I3	If any personal data breach occurred, the data processor informed the data controller without undue delay after having become aware of such personal data breach at the data processor or a subprocessor.	We have inspected that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach.	We have been informed that there have been no breaches during the period. No deviations noted.

I4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency: • Nature of the personal data breach • Probable consequences of the personal data breach • Measures taken or proposed to be taken to respond to the personal data breach.	We have inspected 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 • Describing the probable consequences of the personal data breach • Describing measures taken or proposed to be taken to respond to the personal data breach.	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."

Casper Langhoff (CVR valideret)
Enreach Campaigns A/S CVR: 31073103
Direktør
Serienummer: e4fc44e3-48d1-42ad-b0a6-4f370c36b11c
IP: 95.166.xxx.xxx
2026-01-12 12:41:47 UTC

Michael Mortensen (CVR valideret)
Roesgaard Godkendt Revisionsaktieselskab CVR: 37543128
Statsautoriseret revisor
Serienummer: 56c78f0d-d030-41dc-a7fe-ad94bcba5a88
IP: 185.98.xxx.xxx
2026-01-12 12:51:13 UTC