Admincontrol Privacy Statement Platform

Classification: Public

This Privacy Statement was last updated in **January 2026.**

Table of contents

1. Introduction and scope

Admincontrol AS ("Admincontrol", "we", "us", or "our") is a company registered in Norway under organisation number 987 992 883, with its registered office at Dronning Mauds gate 3, 0250 Oslo, Norway. Admincontrol is part of the Euronext Group.

This Platform Privacy Statement describes how personal data is collected, used, and protected when you use the:

- Admincontrol Platform (app.admincontrol.net), including all connected or integrated applications and modules; and
- features, configuration tools, support services, and other components that form part of the Admincontrol Service.

This statement applies to personal data processed:

- as Data Processor – where Admincontrol processes personal data on behalf of its Customers (the Data Controllers) in connection with their use of the Admincontrol Platform; and
- as Data Controller – for limited categories of personal data that Admincontrol processes for its own purposes in connection with the Admincontrol Platform, such as platform security monitoring, service diagnostics, account administration, and management of optional features (including AI-assisted functionality).

This Platform Privacy Statement is designed to meet the requirements of the General Data Protection Regulation (EU) 2016/679 (GDPR), the UK GDPR, and applicable national laws, including the Norwegian Personal Data Act. Terms used in this statement shall have the same meaning as defined in Article 4 GDPR unless otherwise specified.

2. Roles and responsibilities

2.1 When we act as Data Processor

For the Admincontrol Service, Admincontrol AS acts as Data Processor when processing personal data on behalf of its Customers. In this role, the Customer determines the purposes and means of the processing and is the Data Controller for all personal data uploaded to, generated within, or otherwise processed through the Admincontrol Board Management Platform or Data Room environments. A Data Processing Agreement (DPA) forms part of every customer subscription and governs the processing activities carried out by Admincontrol. The DPA incorporates the requirements of Articles 28 and 32 GDPR, including obligations relating to confidentiality, security, sub-processor management, assistance with data-subject rights, and audit.

Scope of Processor Activities

In its capacity as Data Processor, Admincontrol processes personal data solely for the purpose of delivering and maintaining the Admincontrol Service, including:

- user authentication, access control, and account administration;

- secure hosting, storage, and presentation of customer documents and data;
- collaboration, communication, workflow, and board-meeting management features;
- audit logging, traceability, and platform activity monitoring; and
- provision of customer support and technical assistance.

Admincontrol processes personal data only on the Customer's documented instructions, as set out in the DPA, the Terms of Service, and the functionality chosen by the Customer. Admincontrol does not determine the content, accuracy, or lawfulness of customer-uploaded data.

Platform Security and Operational Integrity

Certain processing must be carried out by Admincontrol to ensure the security, integrity, and availability of the platform, including:

- incident detection and investigation;
- protection against misuse or unauthorised access;
- system monitoring, diagnostics, and error resolution; and
- maintaining service continuity and resilience.

These activities are necessary to operate a secure SaaS platform and are performed under Admincontrol's legitimate interest (Article 6(1)(f) GDPR) in ensuring platform reliability and safeguarding customer data. Such processing is strictly limited to what is necessary and never involves using customer data for independent commercial purposes, profiling, or marketing.

Product improvement and aggregated insights

Where expressly permitted under the DPA or other contractual documentation, Admincontrol may process limited technical or usage data for compatible internal purposes, such as:

- performance optimisation and capacity planning;
- service quality improvements;
- production of aggregated or pseudonymised analytics that do not identify individuals.

Any such processing is:

- strictly controlled,
- subject to role-based access restrictions,
- carried out without examining or reusing customer content, and
- compliant with applicable data-protection laws and contractual commitments.

2.2 When we act as Data Controller

Admincontrol AS acts as Data Controller for certain categories of personal data that it processes for its own purposes and not on behalf of a customer. This applies primarily to personal data processed through:

- the Admincontrol websites and associated digital marketing channels;
- demo, pricing, or contact requests submitted through online forms;
- event, webinar, or newsletter registrations;
- customer feedback surveys and other user-initiated interactions; and
- administrative and security activities necessary to operate and protect the Admincontrol platform.

In these contexts, Admincontrol determines the purposes and means of processing and is responsible for ensuring compliance with applicable data-protection laws.

Purposes of Processing

As Data Controller, Admincontrol processes personal data to:

- respond to enquiries and provide requested information;
- manage sales, marketing, and customer-relationship activities;
- administer events, webinars, and related communications;
- gather feedback to improve and develop our services;
- maintain the security, stability, and performance of the Admincontrol platform (e.g., system monitoring, diagnostics, and incident handling); and
- comply with legal and regulatory obligations.

Processing carried out via Admincontrol's public websites (admincontrol.com and related subdomains) is further described in the separate Admincontrol Website Privacy Statement.

Categories of Personal Data

Personal data processed for these purposes may include:

- contact and professional information (name, email address, company, job title, phone number);
- communication history and preferences;
- technical and usage data generated by interactions with our websites or platform interfaces (e.g., device information, session metadata, logs, diagnostics);
- marketing or event-registration details; and
- feedback or survey responses.

Legal Basis

We rely on one or more lawful bases under the GDPR, including performance of a contract, legal obligation, legitimate interest and, where required, your consent. Further details and examples of these legal bases are provided in section 4 – Lawful basis for processing.

3. Personal data we process

As described in section 2.1 – When we act as Data Processor, Admincontrol processes personal data on behalf of the Customer in connection with the Admincontrol Board Management Platform and Data Room environments. This section summarises the main categories of personal data that may be processed within the Service.

Categories of personal data processed as Data Processor

Admincontrol may process the following categories of personal data on behalf of the Customer:

- **User account and access data**
  Name, business email address, phone number, job title, organisation, and login credentials (including encrypted passwords or eID identifiers used to connect personal electronic identification to the Admincontrol user account).
- **Platform and collaboration data**
  Documents, messages, comments, files, and any other content uploaded, created, shared, or stored within the platform's modules (e.g., Board Portal, Data Room).
- **Audit and activity logs**
  User actions, timestamps, file history, session identifiers, and system metadata required for traceability, compliance, governance workflows, and security monitoring.
- **Support and service data**
  Information submitted through support requests, incident reports, diagnostics, and related correspondence.

Special categories of personal data

The Admincontrol Service is not intended for processing special categories of personal data under Article 9 GDPR. If a Customer chooses to upload such data, the Customer as Data Controller is responsible for ensuring that an appropriate lawful basis under Article 9(2) or Article 10 GDPR applies.

Admincontrol processes this data only on the Customer's documented instructions and for the purpose of providing, maintaining, and securing the Admincontrol Service. Admincontrol does not use Customer Data for independent purposes such as marketing, profiling, or commercial analytics. Certain technical metadata (such as authentication logs and telemetry) may also be processed by Admincontrol as an independent Data Controller for security and performance purposes, as described in sections 2.1 and 4.

4. Lawful basis for processing

Admincontrol processes personal data on one or more lawful bases under the GDPR, depending on the context in which the data is processed and whether Admincontrol acts as Data Processor (on behalf of the Customer) or Data Controller (for platform operations, security, diagnostics, and limited administrative purposes).

The table below outlines the lawful bases most relevant to the Admincontrol Service.

Lawful basis	**Description**	**Examples of platform processing activities**
Performance of a contract (Article 6(1)(b) GDPR)	Processing is necessary to deliver the Admincontrol Service in accordance with the customer's subscription agreement and to fulfil Admincontrol's contractual obligations.	• Providing and operating the Board Portal and Data Room. • User authentication and access control. • Managing roles, permissions, and account configuration. • Enabling secure document hosting, collaboration, and meeting workflows. • Providing customer support and resolving technical issues.
Legal obligation (Article 6(1)(c) GDPR)	Processing is required by law, including obligations relating to security, audit, corporate governance, financial reporting, and regulatory compliance.	• Maintaining mandatory system logs for security and audit purposes. • Compliance with statutory record-keeping obligations. • Cooperating with supervisory authorities or responding to lawful requests.
Legitimate interest (Article 6(1)(f) GDPR)	Processing is necessary for Admincontrol's legitimate interests in operating a secure, reliable, and efficient SaaS platform, provided these	• Protecting the integrity, confidentiality, and availability of the platform

	interests do not override the rights of users.	• Detecting, investigating, and preventing misuse, fraud, or security incidents. • Performing diagnostics, service monitoring, and system performance analysis. • Conducting aggregated, pseudonymised analytics to improve service stability and resilience. • Operating limited controller-level processing for security logs, telemetry, and operational metadata.

Legitimate interest assessments

Where Admincontrol relies on legitimate interest, we ensure that:

- the processing is proportionate and necessary;
- the impact on individuals is minimal;
- appropriate safeguards (e.g., access controls, pseudonymisation, or aggregation) are applied; and
- the rights and freedoms of data subjects are not overridden.

Individuals may object to processing based on legitimate interest at any time (see Section 10 – Data subject rights).

5. Data collection and international transfers

5.1 Data collection

Admincontrol collects personal data only to provide, maintain, and support the secure and reliable operation of the Admincontrol Service. The manner in which personal data is collected depends on how users and Customers interact with the platform.

1. Directly from users

Personal data may be provided directly by users when they:

- create, activate, or access a user account;
- upload, view, or share documents, comments, or other materials within the platform;

- participate in meetings or workflows;
- submit information through forms within the platform; or
- communicate with Admincontrol's support teams.

2. Indirectly from Customers

Authorised Customer administrators may provide personal data when they:

- invite or register new users (e.g., board members, management, advisors, external collaborators);
- assign roles, permissions, or access levels;
- upload documents or content that includes personal information.

In these cases, the Customer acts as Data Controller and is responsible for ensuring that a valid lawful basis applies and that individuals are appropriately informed.

3. Automatically through technical means

When the platform is accessed, Admincontrol automatically processes limited technical data necessary for security, authentication, and service functionality. This may include:

- device, browser, and connection information;
- authentication and session identifiers;
- platform usage telemetry;
- audit-trail metadata required for traceability and compliance.

Technical logging and audit data processed inside the platform is performed under Admincontrol's legitimate interest in ensuring platform integrity, security, and performance.

5.2 Data storage and location

All Customer Data processed through the Admincontrol Service is stored in secure data centres located within the European Economic Area (EEA). Admincontrol applies a comprehensive set of technical and organisational measures to ensure the confidentiality, integrity, and availability of Customer Data throughout its lifecycle.

These measures form part of the ISO/IEC 27001-certified Information Security Management System (ISMS).

Our security framework includes, among other controls:

- **rigorous access control**, based on the principle of least privilege;
- **encryption** of data in transit and at rest;
- **network and infrastructure protection**, including firewalls, intrusion detection, and continuous monitoring;

- **redundancy and resilience measures** to ensure high availability; and
- **regular audits, penetration testing, and risk assessments** in line with ISO/IEC 27001 and industry best practices.

Admincontrol does not host Customer Data outside the EEA unless explicitly instructed by the Customer and only where appropriate safeguards under Chapter V GDPR are in place.

5.3 International transfers

In limited circumstances, certain personal data may be accessed from or transferred to countries outside the European Economic Area (EEA). This may occur, for example:

- when authorised users access the Admincontrol Service from outside the EEA;
- when a specialist support provider or sub-processor operates from a third country; or
- where you have provided documented instructions or consent for a specific processing activity.

Any such transfer is carried out only where necessary and always under conditions that ensure a level of protection essentially equivalent to that guaranteed within the EEA.

To achieve this, Admincontrol implements appropriate safeguards in accordance with Chapter V GDPR, including:

- the European Commission's Standard Contractual Clauses (SCCs) for international data transfers; and
- supplementary technical and organisational measures, such as encryption, strict access control, and data-minimisation practices.

These controls ensure that Customer Data remains protected to GDPR standards, regardless of where it is accessed or processed.

6. Sharing and disclosure of personal data

As your Data Processor, Admincontrol shares personal data only where necessary to deliver the Admincontrol Service, comply with legal or regulatory requirements, or operate the platform securely and efficiently. All sharing takes place strictly in accordance with your documented instructions, the applicable contractual documentation (including the DPA), and this privacy statement.

Personal data may be disclosed to the following categories of recipients:

- **Service providers and sub-processors**

Third-party providers engaged to deliver hosting, infrastructure, maintenance, technical support, security monitoring, or other essential operational services required for the Admincontrol platform. A current and regularly updated list of approved sub-processors is

available at: https://admincontrol.com/sub-processors-sub-contractors

All sub-processors operate under written agreements that include the safeguards required by Articles 28 and 46 GDPR.

- **Euronext Group entities**

Admincontrol may share limited personal data with other entities within the Euronext Group of companies, of which it forms part, where necessary for centralised administrative, legal, IT, security, and group-level marketing and sales-support functions. Such intra-group processing may include, for example, centralised CRM management, lead management and routing, coordination of B2B marketing campaigns (including event follow-up), and customer relationship management, as well as compliance, billing, internal reporting, and service administration.

Such intra-group processing occurs on a documented need-to-know basis and under strict contractual safeguards, including intra-group data-transfer agreements and, where applicable, Standard Contractual Clauses (SCCs). Where intra-group sharing supports marketing communications, Admincontrol will ensure that such communications are sent only where legally permitted (and, where required, subject to your consent), and you can opt out at any time. This sharing is based on legitimate interest (Article 6(1)(f) GDPR) to ensure operational efficiency and consistent governance across the Euronext Group.

- **Public authorities**

Personal data may be disclosed where required to comply with applicable laws, lawful requests, court orders, audits, or regulatory investigations. Admincontrol assesses the scope and legality of all such requests before disclosing any data.

- **Corporate transaction participants**

In the context of a potential or actual merger, acquisition, reorganisation, or divestiture involving Admincontrol AS or any Euronext Group entity, relevant personal data may be shared with advisors, counterparties, or acquiring entities. Such disclosures are subject to strict confidentiality obligations and ongoing data-protection requirements aligned with the GDPR.

All recipients of personal data are bound by contractual or statutory confidentiality and are required to implement appropriate technical and organisational measures to ensure the protection of personal data in accordance with the GDPR and applicable law.

7. Data retention

Admincontrol retains personal data only for as long as necessary to fulfil the purposes for which it was collected, to comply with applicable legal or regulatory obligations, or as otherwise instructed by the Customer. Retention periods depend on the type of data and the context in which it is processed.

- **Customer and user account data**

Retained for the duration of the contractual relationship and securely deleted or anonymised within a defined period after termination, unless a longer retention period is required by law or necessary to establish, exercise, or defend legal claims.

- **Log and support metadata**

Retained for a limited period strictly necessary to ensure platform security, perform diagnostics, support incident investigations, and maintain system auditability.

Customer control over retention

Where Admincontrol processes Customer Data as Data Processor, the Customer acting as the Data Controller determines the applicable retention periods. Admincontrol follows these documented instructions and ensures that, after expiry of the relevant period, Customer Data is securely deleted or irreversibly anonymised in accordance with GDPR requirements and recognised industry standards.

8. Data security

Admincontrol applies a comprehensive set of technical and organisational measures to ensure the confidentiality, integrity, and availability of personal data processed through the Admincontrol platform. These controls form part of the ISO/IEC 27001-certified Information Security Management System (ISMS) operated by Admincontrol.

Key security measures

- **Encryption**
  All personal data is encrypted both in transit and at rest using industry-standard protocols (e.g. TLS, AES-256). This protects data against unauthorised access during transmission and storage.
- **Access control**
  Access to personal data is strictly limited to authorised personnel with a defined operational need. Role-based access controls, authentication mechanisms, and least-privilege principles are applied across all systems.
- **Monitoring, testing, and hardening**
  The platform undergoes continuous monitoring, regular vulnerability assessments, and independent penetration testing to ensure ongoing resilience and to identify and address potential threats proactively.
- **Secure development and change management**
  Platform updates, enhancements, and configuration changes follow controlled development and release processes that incorporate security-by-design and secure coding principles.
- **Business continuity and incident response**
  Admincontrol maintains tested procedures for backup, disaster recovery, and security-

incident response, including obligations under Articles 33–34 GDPR. Security events are managed through established escalation and reporting workflows.

- **Certified governance framework**
  Admincontrol operates within the ISO/IEC 27001-certified ISMS of Admincontrol AS demonstrating adherence to internationally recognised standards for information security, risk management, and operational governance.

Shared responsibility

While Admincontrol implements extensive security safeguards, Customers also play a key role in protecting personal data. We strongly encourage the use of complementary measures such as:

• robust user-access governance and role management;
• multi-factor authentication (MFA) for all users;
• strong password and device-security policies; and
• internal procedures for reviewing access rights and managing user lifecycle events.

Contractual security obligations

Additional details on Admincontrol's security commitment including audit rights, breach-notification procedures, incident-response timelines, and sub-processor controls are set out in the applicable Data Processing Agreement (DPA) and associated documentation.

9. Cookies and tracking technologies

Admincontrol uses cookies and similar technologies to ensure secure access, maintain session continuity, and improve user experience across its websites and connected applications. These technologies help us deliver essential platform functions and, where consent is provided, enhance site performance and personalisation.

Types of cookies used

- **Strictly necessary cookies** – Required for authentication, security, and core functionality of the platform. These cookies enable login sessions, access to secure areas, and proper service operation.
- **Functional cookies** – Allow the website to remember user preferences, such as language or regional settings, to provide a more consistent experience.
- **Analytical cookies** – Used to analyse site performance, understand user behaviour, and improve functionality. Data collected through these cookies is aggregated and pseudonymised.
- **Marketing cookies** – Used only with your prior consent to deliver personalised content, advertising, or relevant communications based on your interaction with our websites.

A detailed overview of cookies including their purpose, duration, and technical details is provided in Annex 2 – Cookie Inventory. You may manage or update your cookie preferences at any time via the “Cookie Settings” link or by clearing cookies in your browser. Guidance for manual cookie removal is provided in Annex 3 – How to Remove Cookies.

Legal basis

The use of strictly necessary cookies is based on our legitimate interest under Article 6(1)(f) GDPR to ensure secure, functional, and user-friendly service delivery. For all other categories of cookies including functional, analytical, and marketing cookies we rely on your consent in accordance with Article 6(1)(a) GDPR and the EU ePrivacy Directive.

10. Data subject rights

As a data subject, you have several rights under the General Data Protection Regulation (GDPR) in relation to the personal data processed through the Admincontrol platform and related services. These include:

- **Right of access:** to request confirmation of whether your personal data is being processed and to obtain a copy of the data concerned.
- **Right to rectification:** to request the correction of inaccurate or incomplete personal data.
- **Right to erasure:** to request the deletion of personal data where it is no longer necessary for the purposes for which it was collected or where there is no lawful basis for continued processing.
- **Right to restriction of processing:** to request that processing be temporarily limited for example, while the accuracy of data is being verified.
- **Right to object:** to object to processing based on our legitimate interests, unless we can demonstrate compelling legitimate grounds to continue processing.
- **Right to withdraw consent:** where processing is based on consent, you may withdraw it at any time without affecting the lawfulness of processing prior to withdrawal.
- **Right to data portability:** where applicable, to receive your personal data in a structured, commonly used, and machine-readable format, or to have it transmitted directly to another controller.

Please note that certain rights may be limited where personal data must be retained or processed to comply with legal or regulatory obligations for example, statutory record-keeping, audit, or contractual requirements necessary to maintain service integrity. To exercise your rights or submit a request, please contact the ECS Data Protection Officer at:

By email: dpo.ecs@euronext.com
By post:

Attn. Data Protection Officer
14, place des Reflets – CS30064
92054 Paris La Défense, France

We may ask you to verify your identity before responding to your request, in accordance with our internal verification procedures.

11. Artificial Intelligence (AI) features

This section governs the use of artificial intelligence-enabled functionalities ("AI functionalities") made available within the Admincontrol platform. It supplements this Privacy Statement and the applicable Data Processing Agreement. AI functionalities are designed and deployed as decision-support tools and are not intended to constitute high-risk or safety-critical systems. This section applies to personal data processed through AI functionalities provided by Admincontrol. AI functionalities may be offered across different Admincontrol products, including the Board Management Portal and the Virtual Data Room.

AI functionalities are designed to support users through automated assistance such as drafting, summarisation, and search and retrieval of content. They do not make autonomous decisions and operate solely based on user instructions.

11.1 Scope of AI functionalities

Depending on the product and configuration, AI functionalities may include, among others:

- an AI Assistant supporting drafting, summarisation, and contextual assistance within the Board Management Portal; and
- AI-powered search capabilities enabling users to locate and retrieve information within documents and data rooms.

The availability and specific functionality of AI features may vary per product and over time.

11.2 Roles and responsibilities

- **Customer as Data Controller**
  When using AI functionalities, the Customer remains the Data Controller for all personal data entered into, accessed by, or generated through these features and must ensure a valid legal basis for processing under the GDPR.
- **Admincontrol as Data Processor**
  Admincontrol processes personal data solely on the Customer's documented

instructions and only to provide, operate, support, and maintain the AI functionalities in accordance with the applicable contractual documentation.

In limited cases, Admincontrol may process certain usage and technical metadata (such as timestamps, request logs, or performance metrics) as an independent Data Controller, based on its legitimate interest under Article 6(1)(f) GDPR, to ensure the availability, integrity, and security of the AI functionalities.

11.3 Data handling and security

- All AI-related processing takes place within Admincontrol's ISO/IEC 27001-certified Information Security Management System (ISMS).
- Inputs and outputs are encrypted both in transit and at rest.
- Personal data processed through AI functionalities is not used to train, retrain, or improve external or third-party AI models.
- AI outputs are generated in real time and are not retained beyond what is necessary for operational logs, support, audit, or security purposes.
- Sub-processors involved in supporting AI functionalities are listed at https://admincontrol.com/sub-processors-sub-contractors and are subject to GDPR-compliant contractual safeguards.

11.4 User responsibilities and limitations

Customers and users must:

- avoid entering special categories of personal data (Article 9 GDPR) or other highly sensitive or confidential information unless strictly necessary and legally justified;
- review and validate AI-generated outputs prior to use, as AI functionalities provide decision-support only and do not constitute legal, financial, or professional advice;
- use AI functionalities exclusively for lawful, organisation-related purposes and in accordance with applicable internal governance policies.

11.5 Transparency and audit

Admincontrol maintains audit and security logs related to the use of AI functionalities for compliance, monitoring, and security purposes. Upon request, Customers may obtain additional information regarding applicable technical and organisational measures, data flows, or risk assessments relating to the AI functionalities.

11.6 Future AI functionalities

Admincontrol may, from time to time, develop and make available additional artificial intelligence-enabled functionalities within the Platform (“future AI functionalities”). Such future AI functionalities may support new or expanded use cases, features, or products and may be introduced progressively.

Unless explicitly stated otherwise:

- future AI functionalities will be subject to this Privacy Statement and the applicable Data Processing Agreement;
- the allocation of roles and responsibilities between the Customer and Admincontrol as Data Controller and Data Processor will follow the same principles set out in this section;
- personal data processed through future AI functionalities will be subject to appropriate technical and organisational measures designed to ensure a level of security appropriate to the risk; and
- future AI functionalities will not operate autonomously or independently of user interaction.

Where the introduction of a future AI functionality results in a material change to the nature, scope, or purposes of the processing of personal data, Admincontrol will provide appropriate information to Customers in advance, and, where required, update the relevant contractual or privacy documentation.

12. Updates to this privacy statement

This privacy statement may be updated from time to time to reflect changes in our processing activities, applicable legal requirements, or technological developments. The most recent version will always be available on the Admincontrol platform and website. Where material changes are made that significantly affect the way personal data is processed, we will provide appropriate notice through the platform or other direct communication channels before the changes take effect.

Annex 1 – Glossary of terms

Term	Definition
AI Addendum	A contractual supplement, where applicable, governing the use of certain AI functionalities within the Admincontrol Platform. The AI Addendum forms part of the Customer’s agreement with

	Admincontrol and defines specific responsibilities, permitted use, and data-protection safeguards for designated AI features.
Customer	The organisation or entity that has entered into a subscription or service agreement with Admincontrol AS for use of the Admincontrol Platform. The Customer acts as the Data Controller for personal data processed within the platform.
Data Controller	The natural or legal person, public authority, agency, or other body that determines the purposes and means of the processing of personal data (Article 4(7) GDPR). In the context of the Admincontrol Service, the Customer acts as the Data Controller.
Data Processor	The natural or legal person, public authority, agency, or other body that processes personal data on behalf of the Data Controller (Article 4(8) GDPR). Admincontrol acts as the Data Processor when providing, supporting, and maintaining the platform on behalf of its Customers.
Data Subject	An identified or identifiable natural person whose personal data is processed by a Data Controller or Data Processor for example, platform users, Customer employees, board members, or other individuals whose data is processed through the Service.
European Economic Area (EEA)	The Member States of the European Union together with Iceland, Liechtenstein, and Norway. Transfers of personal data outside the EEA are subject to the safeguards set out in Chapter V GDPR.
Euronext Corporate Services B.V. (ECS B.V.)	An affiliated company within the Euronext Group, certified to ISO/IEC 27001, that operational support for Admincontrol and other Euronext Corporate Services platforms.
GDPR	The General Data Protection Regulation (EU) 2016/679, which governs the protection of personal data and the rights of individuals within the European Union and EEA.
Information Security Management System (ISMS)	A comprehensive framework of policies, procedures, and controls designed to manage information-security risks. The ISMS operated by Admincontrol is certified to ISO/IEC 27001.
Personal Data	Any information relating to an identified or identifiable natural person, such as name, email address, identification number, online identifier, or other data that can be linked directly or indirectly to an individual.
Processing	Any operation or set of operations performed on personal data, whether or not by automated means such as collection, recording,

	organisation, storage, alteration, retrieval, consultation, use, disclosure, or deletion.
Standard Contractual Clauses (SCCs)	Contractual safeguards adopted by the European Commission to ensure that personal data transferred outside the EEA receives an adequate level of protection consistent with the GDPR.
Sub-processor	A third-party service provider engaged by Admincontrol to process personal data on behalf of its Customers and in accordance with documented instructions.

Annex 2 – Cookie Inventory

The tables below list the cookies that may be used across Admincontrol's websites and connected applications. Cookies are grouped by purpose, with details on name, domain, type, expiry, and purpose. This inventory is updated periodically to reflect current usage.

1. Essential Cookies

Cookie Name	Domain / Subgroup	Type	Expiry	Purpose
*******-seap-****-****	*.admincontrol.net	First Party	Session	This cookie is associated with the private cloud load balancing service. The cookie is used to ensure traffic and user data is routed to the correct locations where a site is hosted on multiple servers, so that the end user has a consistent experience.
*******- 1pap-****-****	*.admincontrol.net	First Party	Session	This cookie is associated with the private cloud

				load balancing service. The cookie is used to ensure traffic and user data is routed to the correct locations where a site is hosted on multiple servers, so that the end user has a consistent experience.
.AspNetCore.	login.admincontrol.net	First Party	Session	Maintains session state for secure access.
.AspNetCore.Antiforgery	login.admincontrol.net	First Party	Session	Anti-forgery cookie set by web applications. It is designed to stop unauthorised posting of content to a website, known as Cross-Site Request Forgery. It holds no information about the user and is destroyed on closing the browser.
.AspNetCore.Mvc.CookieTempDataProvider	*.admincontrol.net	First Party	Session	strictly necessary session cookie to temporarily store data (known as TempData).

.AspNetCore.Session	*.admincontrol.net	First Party	Session	Maintains session state for secure access.
.AspNetCore.Session-fallback	*.admincontrol.net	First Party	Session	Maintains session state for secure access.
__Host-AuthCookie	*.admincontrol.net	First Party	Session	Used for facilitating user authentication.
__Host-idsrv	*.admincontrol.net	First Party	Session	To facilitate authentication
__Host-SessionId	*.admincontrol.net	First Party	Session	Maintains session state for secure access.
__RequestVerificationToken	app.eu.admincontrol.net	First Party	Session	Anti-forgery cookie set by web applications. It is designed to stop unauthorised posting of content to a website, known as Cross-Site Request Forgery. It holds no information about the user and is destroyed on closing the browser.
ARRAffinity	app.eu.admincontrol.net	First Party	Session	Used for load balancing to make sure the visitor page requests are routed to the same server in any browsing session.
ARRAffinitySameSite	app.eu.admincontrol.net	First Party	Session	Used for load balancing to

				make sure the visitor page requests are routed to the same server in any browsing session.
fileDownload	*.admincontrol.net	First Party	Session	Used for detection when a file download ends
idsrv.session	*.admincontrol.net	First Party	Session	Maintains session state for secure access.
JSESSIONID, fallback, transid	signing.admincontrol.net	First Party	Session	session cookie, used by our software provider for signing services. Used to maintain an anonymous user session by the server.
NSC_xxxxxxxxxxxxxxx	login.admincontrol.net	First Party	Session	This cookie is associated with the private cloud load balancing service. This is a pattern type cookie with the root being NSC_ and the rest of the name being a unique encrypted alpha numeric identifier for the virtual server it originated from. The cookie is used to ensure

				traffic and user data is routed to the correct locations where a site is hosted on multiple servers, so that the end user has a consistent experience.
TiPMix	*.cloud.admincontrol.net	First Party	Session	Used for load balancing across user sessions for public cloud offerings
update-token	*.admincontrol.net	First Party	Session	Notifies the client for the need to refresh its CSRF tokens
x-ms-routing-name	*.cloud.admincontrol.net	First Party	Session	Used for load balancing across user sessions for public cloud offerings
AUTH_SESSION_ID, KC_RESTART, KEYCLOAK_IDENTITY	auth.bankid.no	Third Party	Session	Used for facilitating authentication using eID
refresh_gui	login.bankid.no, auth.bankid.no			Used for facilitating authentication using eID
BIDCID	csfe.bankid.no	Third Party	Session	Used for facilitating authentication using eID
user_ai, user_rb	app.bankid.no	Third Party	Session	Used for security and fraud prevention
transId, SESSION, idsrv.external, idsrv.session, idsrv	eid.admincontrol.net	Third Party	Session	Used for electronic signing

2. Functional Cookies

Cookie Name	Domain / Subgroup	Type	Expiry	Purpose
OptanonAlertBoxClosed	login.admincontrol.net	First Party	Persistent	This cookie is set by websites using certain versions of the cookie law compliance solution from OneTrust. It is set after visitors have seen a cookie information notice and, in some cases, only when they actively close the notice down. It enables the website not to show the

				message more than once to a user. The cookie has a normal lifespan of one year and contains no personal information.
OptanonConsent	login.admincontrol.net	First Party	Persistent	This cookie is set by websites using certain versions of the cookie law compliance solution from OneTrust. It is set after visitors have seen a cookie information notice and in some cases only

				when they actively close the notice down. It enables the website not to show the message more than once to a user. The cookie has a normal lifespan of one year and contains no personal information.
ConsentResponse.xxxxxxxxxxxxxx	login.admincontrol.net	First Party	Session	Used by website cookie management systems to record a user's choice
OpenIdConnect.nonce.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	login.admincontrol.net	First Party	Persistent	This cookie is set by website

				s using certain versions of the cookie law compliance solution from OneTrust. It is set after visitors have seen a cookie information notice and, in some cases, only when they actively close the notice down. It enables the website not to show the message more than once to a user. The cookie has a normal lifespan of

				one year and contains no personal information.
sidebarmenu	*.admincontrol.net	First Party	Session	Used to toggle the sidebar to collapsed vs expanded.
topbarsmallmenu	*.admincontrol.net	First Party	Session	Toggles its value when the screen gets too small.

3. Analytical Cookies

Cookie Name	**Domain / Subgroup**	**Type**	**Expiry**	**Purpose**
NPS_EU-********_last_seen	*.admincontrol.net	First Party	Session	To analyse site performance, understand user behaviour, and improve functionality. Data collected through these cookies is aggregated and pseudonymised.
NPS_EU-********_ surveyed	*.admincontrol.net	First Party	Session	To analyse site performance, understand user behaviour, and improve functionality. Data collected through these cookies is aggregated and pseudonymised.
NPS_EU-********_ throttle	*.admincontrol.net	First Party	Session	To analyse site performance, understand user behaviour, and

				improve functionality. Data collected through these cookies is aggregated and pseudonymised.

4. Marketing Cookies

None

Legal Basis and Consent

- The use of strictly necessary cookies is based on legitimate interest under Article 6(1)(f) GDPR to ensure secure and functional service delivery.
- All other cookies (functional, analytical, and marketing) are used only with the user's consent under Article 6(1)(a) GDPR.
- You may manage or withdraw your consent at any time via the "Cookie Settings" link or by clearing cookies from your browser.

For instructions on manual cookie removal, see Annex 3 – How to Remove Cookies.

Annex 3 – How to Remove Cookies

To remove or disable cookies, you can adjust your browser settings. The following links provide guidance for commonly used browsers:

- **Google Chrome:** Clear, enable, and manage cookies in Chrome
- **Mozilla Firefox:** Clear cookies and site data in Firefox
- **Microsoft Edge:** View and delete browser history in Microsoft Edge
- **Safari:** Manage cookies and website data in Safari

You may also delete all cookies from your device at any time by clearing your browser's cache. Please note that removing essential cookies may impact website functionality.