CTC Portal Privacy Notice

Operator	Nordic Consult 2026 ApS
CVR	DK46679717
Version	1.0
Effective date	2026-10-07
Registered address	Knud Rasmussens Vej 11, 2870 Dyssegård, Denmark
Legal and privacy contact	support@nordicconsult.dk

1. Data controller

Nordic Consult 2026 ApS, CVR DK46679717, is the data controller for personal data processed in connection with Portal accounts, usage, communications and administration.

Contact details:

- Address: Knud Rasmussens Vej 11, 2870 Dyssegård, Denmark
- Email: support@nordicconsult.dk

2. Personal data we process

Depending on use of the Portal, we may process:

- identity and contact data: first name, last name, job title, email address and phone number;
- organisation data: company name, company association and account status;
- account and security data: authentication identifiers, verification status, login and session data, IP address, device/browser information and security events;
- usage data: CTC pages and content sections viewed, timestamps, searches, links or documents opened and other interaction events;
- subscription data: subscribed CTC areas, subscription changes, last visits and unread-change state;
- communication data: support messages, service notifications, delivery status and marketing choices;
- privacy-request data: access, export, correction, objection, consent withdrawal and deletion requests; and
- consent evidence: the wording, channel, timestamp, source and status of any optional consent.

Do not submit special-category personal data, confidential client data or tax records through the Portal unless Nordic Consult has expressly approved a secure and lawful process for doing so.

3. Purposes and legal bases

Purpose	Principal legal basis
Create and administer accounts; provide requested Portal functions	GDPR Article 6(1)(b), where the user is party to the arrangement; otherwise Article 6(1)(f), our legitimate interest in providing the B2B service to the customer's authorised users
Authenticate users, secure the Portal, prevent misuse and investigate incidents	Article 6(1)(f), legitimate interests in security and fraud prevention; Article 6(1)(c) where a legal obligation applies

Purpose	Principal legal basis
Record subscriptions and send requested CTC-area or account notifications	Article 6(1)(b) and/or Article 6(1)(f), depending on the user relationship
Provide support and respond to requests	Article 6(1)(b), Article 6(1)(f), or Article 6(1)(c) for statutory privacy requests
Produce company-level usage analysis and improve the Portal	Article 6(1)(f), legitimate interests in service operation, improvement and understanding customer use, subject to access controls and balancing of user rights
Send promotional email or make marketing calls where consent is required	Article 6(1)(a), consent, together with applicable Danish marketing rules
Establish, exercise or defend legal claims and document compliance	Article 6(1)(f) and, where applicable, Article 6(1)(c)

Where processing relies on legitimate interests, users may object for reasons relating to their particular situation. Where processing relies on consent, consent may be withdrawn at any time without affecting processing already carried out lawfully.

4. Sources of data

We generally receive data directly from the user, the user's company and the user's interaction with the Portal. Security and delivery information may also be received from our hosting, authentication and email providers.

5. Recipients and processors

Access within Nordic Consult is limited to authorised personnel who need the data for administration, support, security, legal compliance or approved customer-activity analysis.

The current principal service providers are:

Provider	Function	Location and transfer note
Supabase	Database, authentication and related backend services	The production project must be configured in a selected EU region. Provider support and subprocessors may still involve processing outside the EEA; the applicable DPA and transfer mechanism must be verified before launch.
Vercel	Application hosting, delivery network, logs and deployment infrastructure	Processing may occur through an international infrastructure and subprocessors. Nordic Consult must maintain an appropriate DPA and lawful transfer safeguards for any non-EEA processing.
Resend	Transactional and, where separately consented, marketing email delivery	Email may be routed from Ireland, but Resend states that account data, email metadata, logs and API records are stored in the United States. Nordic Consult must therefore apply the provider DPA and a valid Chapter V transfer mechanism.

We may also disclose data to professional advisers, auditors, public authorities or courts when necessary and lawful, or to a successor in connection with a business transfer subject to appropriate safeguards.

We do not sell personal data.

6. International transfers

Where personal data is transferred outside the European Economic Area to a country not covered by an EU adequacy decision, Nordic Consult will use an appropriate safeguard, such as the European Commission's Standard Contractual Clauses, together with supplementary measures where required. Information about the relevant safeguard may be requested using the privacy contact above.

7. Retention

We retain personal data only for as long as reasonably necessary for the purposes described above and applicable legal requirements. The operational retention schedule is:

Data	Retention criterion
Active account and profile data	While the account is active and for up to 90 days after closure, unless earlier deletion is required or longer retention is legally necessary
Authentication and security logs	Normally up to 12 months; longer when required to investigate or document a security incident
Identifiable usage/activity events	May be retained without a fixed period only after genuine anonymisation or upon deletion request, so that no individual can be reidentified using reasonably available means
Company-level statistics	May be retained without a fixed period only after genuine anonymisation so that no individual can be reidentified using reasonably available means
Support and business correspondence	Normally up to three years after the matter closes, or longer when required for a legal claim
Marketing-consent evidence and withdrawal records	For as long as needed to demonstrate compliance with the applicable consent and limitation rules
Email delivery logs	2 years.
Privacy requests	For the time needed to complete and document the request and satisfy applicable legal obligations

Backups may retain deleted data for a limited period before secure overwrite. Access is restricted and deleted data is not restored except for disaster recovery or legal necessity.

8. Rights

Subject to the conditions in applicable law, a person may request:

- access to personal data;
- correction of inaccurate data;
- deletion;
- restriction of processing;
- data portability where applicable;
- objection to processing based on legitimate interests; and
- withdrawal of consent.

The Portal provides an account-data export and a deletion-request function. Deletion normally anonymises the user's identity while preserving only genuinely anonymised company-level statistics. Nordic Consult may retain data where required by law or necessary for legal claims.

We may need to verify identity and authority before completing a request. A request can also be sent to support@nordicconsult.dk

9. Complaints

Please contact Nordic Consult first so that we can address a concern. A person also has the right to complain to:

Datatilsynet Carl Jacobsens Vej 35 2500 Valby Denmark www.datatilsynet.dk

10. Mandatory and optional information

Profile fields marked as required are necessary to establish and administer an account. If they are not provided, the account may not be created. Optional marketing consent is not required to create or use the Portal.

11. Automated decisions

The Portal does not make decisions producing legal or similarly significant effects solely by automated means. Activity information may be used by authorised Portal administrators to identify potential company interest, but a human must assess any resulting business action.

12. Security

Nordic Consult applies risk-appropriate technical and organisational measures, including access control, authentication, encryption in transit, logging, backup procedures, processor controls and incident handling. No internet service can be guaranteed completely secure.