NCCO

Privacy Policy Supplemental

Including Data Privacy Framework Compliance

Effective Date: October 1, 2026 • Version 1.0

1. Introduction & Scope

National Checking Company, doing business as NCCO ("NCCO," "we," "us," or "our"), is a corporation incorporated and headquartered in the United States and is subject to the investigatory and enforcement power of the Federal Trade Commission. We are committed to protecting the privacy and security of the personal data we process in connection with our business operations.

This Privacy Policy describes how NCCO collects, uses, discloses, and protects personal data relating to our business customers and their designated contacts. It applies to all personal data processed by NCCO in connection with our products and services.

This Policy should be read alongside any applicable Privacy Policy, Data Processing Addendum (DPA) or Master Service Agreement or other agreement (MSA) entered into between NCCO and a customer, which may contain additional or more specific obligations.

For questions about this Policy, please contact:

Privacy Contact	dataprivacy@ncco.com

Mailing Address	NCCO, Attn: Director of IT, 899 Montreal Circle, St Paul, MN, 55102

2. Data We Collect

The list of data we collect is included in the NCCO Privacy Policy https://www.ncco.com/privacy-policy-2/.

3. Purposes & Legal Basis for Processing

NCCO processes personal data for the following purposes:

3.1 Service Delivery

To fulfill our contractual obligations to customers, including provisioning, maintaining, and supporting our products and services. Legal basis: Performance of a contract.

3.2 Account Management

To manage customer accounts, maintain accurate records, and facilitate business communications. Legal basis: Legitimate interests (effective business relationship management).

3.3 Internal Analytics & Product Improvement

To conduct internal reporting, analyze usage patterns, and improve our offerings using anonymized or aggregated analytics. Personal data is processed within our analytics infrastructure (see Section 6 – Subprocessors). Legal basis: Legitimate interests (business improvement and optimization).

3.4 Legal Compliance

To meet applicable legal, regulatory, and contractual obligations, including record-keeping requirements. Legal basis: Legal obligation.

4. Data Privacy Framework (DPF) Compliance

NCCO, including its subsidiary Dot It Restaurant Fulfillment, LLC, complies with the EU-U.S. Data Privacy Framework (EU-US DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-US DPF), as set forth by the U.S. Department of Commerce. NCCO has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. NCCO has also certified that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-US DPF. If there is any conflict between the terms in this Privacy Policy Supplement and the EU-U.S. DPF Principles or Swiss-U.S. DPF Principles (collectively, the “DPF Principles”), the DPF Principles shall govern.

To learn more about the Data Privacy Framework (DPF) Program and to view NCCO’s certification, please visit https://www.dataprivacyframework.gov/.

NCCO’s DPF compliance covers the following Principles:

- Notice – individuals are informed of data collection and use practices
- Choice – individuals may opt out of certain processing and onward transfers
- Accountability for Onward Transfer –NCCO remains liable for subprocessor compliance
- Security – appropriate technical and organizational measures are in place
- Data Integrity & Purpose Limitation – data is limited to specified, compatible purposes
- Access – individuals may access, correct, or delete their personal data
- Recourse, Enforcement & Liability – accessible dispute resolution mechanisms are available

The Federal Trade Commission has jurisdiction over NCCO’s compliance with the DPF Principles. In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

NCCO maintains an internal compliance-verification program to assess, at least annually, its adherence to the applicable DPF Principles and to address identified issues.

5. International Data Transfers

NCCO is headquartered in the United States. Personal data collected from individuals located in the European Economic Area (EEA), United Kingdom (UK), or Switzerland may be transferred to and processed in the United States and other countries where NCCO or its subprocessors operate.

NCCO relies on the following mechanisms to lawfully transfer personal data internationally:

- EU-U.S. Data Privacy Framework (EU-U.S. DPF): primary transfer mechanism for personal data received from the EU/EEA.
- UK Extension to the EU-U.S. DPF: for personal data received from the United Kingdom.
- Swiss-U.S. Data Privacy Framework: for personal data received from Switzerland.
- Standard Contractual Clauses (SCCs): used as a supplementary or fallback mechanism where DPF does not apply, including for transfers to subprocessors that are not DPF-certified.

6. Subprocessors & Onward Transfers

When NCCO transfers personal information received under the DPF to a third party acting as an agent, NCCO enters into a written agreement requiring the agent to process the information only for specified and limited purposes consistent with the individual's consent and the DPF Principles, to provide at least the same level of privacy protection required by the DPF Principles, and to notify NCCO if it can no longer meet that obligation. When NCCO transfers such information to a third party acting as an independent controller, NCCO provides the required notice and choice and enters into an appropriate agreement consistent with the DPF Principles. NCCO remains responsible under the DPF Principles if an agent processes such personal information in a manner inconsistent with the DPF Principles, unless NCCO proves that it is not responsible for the event giving rise to the damage.

NCCO currently engages the following subprocessors that may process customer personal data:

Subprocessor	Purpose	Location	Transfer Mechanism
Snowflake	Data lake / storage for internal analytics	US (Cloud)	DPF / SCCs
Domo	Business intelligence & internal reporting	US (Cloud)	DPF / SCCs
Salesforce	Internal CRM for customer engagement management	US (Cloud)	DPF / SCCs
Microsoft	Azure cloud computing resources	US (Cloud)	DPF / SCCs
Amazon	AWS cloud computing resources	US (Cloud)	DPF / SCCs

NCCO will maintain an up-to-date list of subprocessors and will provide customers with advance notice of material changes to its subprocessor arrangements where required by applicable data processing agreements. Customers who have executed a DPA with NCCO may have the right to object to the addition of new subprocessors in accordance with the terms of that agreement.

NCCO may also disclose personal information to service providers and other third parties that perform services on NCCO's behalf, such as customer-relationship-management, analytics, communications, payment-processing, security, professional-advisory, and legal-compliance providers. NCCO may also disclose personal information where required by law, to protect rights, safety, and security, or in connection with a corporate transaction. The categories and identities of recipients may vary depending on the service and the individual's relationship with NCCO.

7. Data Retention

NCCO retains personal data only for as long as necessary to fulfill the purposes for which it was collected, or as required by applicable law or contract.

- Active customer data is retained for the duration of the customer relationship plus a period of seven (7) years following contract termination, unless a shorter or longer period is required by law.
- Data retained for legal compliance purposes is held for the period required by the applicable law or regulation.
- Where personal data is no longer required, NCCO will securely delete or anonymize it in accordance with its data retention schedule.
- Individual users may request deletion of their cross-ecosystem user accounts at login.ncco.com. Deletion will take place according to the processes and timeframes listed on that site.

8. Data Security

NCCO implements appropriate technical and organizational security measures designed to protect personal data against unauthorized access, disclosure, alteration, or destruction. These measures include, but are not limited to:

- Encryption of personal data in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent)
- Role-based access controls and the principle of least privilege
- Regular security assessments and vulnerability management
- Employee training on data protection and information security

NCCO's subprocessors, including Snowflake, Salesforce, and Domo, maintain their own security certifications (including SOC 2 Type II) and are contractually required to maintain security standards consistent with applicable data protection laws.

In the event of a personal data breach, NCCO will notify affected individuals and relevant supervisory authorities in accordance with applicable law, including within 72 hours of becoming aware of a breach where required by GDPR.

9. Individual Rights

9.1 Rights of EU/EEA, UK, and Swiss Individuals (GDPR & DPF)

Individuals whose personal data is subject to the GDPR or the DPF Principles have the following rights:

- Right of Access – to obtain confirmation of and access to personal data held about you

- Right to Rectification – to request correction of inaccurate or incomplete personal data
- Right to Erasure – to request deletion of personal data in certain circumstances
- Right to Restriction of Processing – to request that processing be limited in certain circumstances
- Right to Data Portability – to receive personal data in a structured, machine-readable format
- Right to Object – to object to processing based on legitimate interests or for direct marketing
- Rights Related to Automated Decision-Making – to not be subject to decisions based solely on automated processing that produce significant legal effects, where applicable

9.2 Rights of US-Based Individuals

US residents may have additional rights under applicable state privacy laws, including the Iowa Consumer Data Protection Act (ICDPA) and, where applicable, the California Consumer Privacy Act (CCPA/CPRA). These may include rights to access, delete, correct, and opt out of the sale or sharing of personal data. NCCO does not sell personal data.

9.3 How to Exercise Your Rights

To exercise any of the rights described in this Section, please submit a request to:

Email	dataprivacy@ncco.com

NCCO will respond to verified requests within 30 days (or as otherwise required by applicable law). NCCO will investigate and respond to complaints concerning its compliance with the applicable DPF Principles within 45 days of receiving the complaint. NCCO may need to verify your identity before processing your request.

10. Choice & Opt-Out (DPF Requirement)

Where NCCO receives personal information subject to the DPF that is considered sensitive information under the applicable DPF Principles, NCCO will obtain affirmative express consent before using or disclosing that information for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual, unless an exception under the DPF Principles applies.

Where NCCO processes personal data for purposes that are materially different from those for which it was originally collected or intends to disclose personal data to a third party acting as a data controller, NCCO will provide individuals with the opportunity to opt out of such processing or disclosure.

To opt out of such uses, please contact dataprivacy@ncco.com. Please note that opting out of certain processing may affect NCCO's ability to provide its services where such processing is necessary for service delivery.

11. Recourse, Enforcement & Dispute Resolution (DPF Requirement)

In compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), NCCO commits to resolve complaints about our collection or use of your personal information transferred to the U.S. pursuant to the EU-U.S. DPF,

the UK extension to the EU-U.S. DPF, and the Swiss-U.S. DPF. EU, UK, and Swiss individuals with inquiries or complaints should first contact NCCO (Attn: Director of IT, 899 Montreal Circle, St Paul, MN, 55102). NCCO will investigate and respond to complaints concerning its compliance with the applicable DPF Principles within 45 days of receiving the complaint.

NCCO has further committed to refer unresolved DPF Principles-related complaints to a U.S.-based independent dispute resolution mechanism, BBB NATIONAL PROGRAMS. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit www.bbbprograms.org/dpf-complaints for more information and to file a complaint. This service is provided free of charge to you.

If your DPF complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See https://www.dataprivacyframework.gov/framework-article/ANNEX-I-introduction for more information.

12. Cookies & Tracking Technologies

NCCO's website and online services may use cookies and similar tracking technologies for essential functionality and analytics purposes. A full description of NCCO's cookie practices, including opt-out options, is available in our Cookie Policy at [URL].

13. Children's Data

NCCO's products and services are directed to business customers and are not intended for use by individuals under the age of 16. NCCO does not knowingly collect personal data from children. If you believe we have inadvertently collected data from a minor, please contact us immediately at dataprivacy@ncco.com.

14. Changes to This Policy

NCCO may update this Privacy Policy from time to time to reflect changes in our practices, legal requirements, or operational needs. When we make material changes, we will notify customers by email and/or by posting a notice on our website at least 30 days prior to the change taking effect. The "Effective Date" at the top of this Policy indicates when the current version took effect.

Continued use of NCCO's products and services following the effective date of an updated Policy constitutes acceptance of the revised terms.

15. Contact Information

For questions, concerns, or to exercise your privacy rights, please contact NCCO using the details below:

Privacy Office (General)	dataprivacy@ncco.com

EU Representative	NCCO, Attn: Karl Rose, Unit A3/A4, Beeches Park, Eastern Avenue, Burton-on-Trent, DE13 0BB, United Kingdom

Mailing Address	NCCO, Attn: Director of IT, 899 Montreal Circle, St Paul, MN, 55102

You also have the right to lodge a complaint with your local data protection supervisory authority. A list of EU supervisory authorities is available at https://www.edpb.europa.eu/about-edpb/about-edpb/members_en. For the UK, please visit: https://ico.org.uk/make-a-complaint/. For Switzerland, please visit: https://www.edoeb.admin.ch/en/contact-2.