

---

## 1. Introduction to the Consumer Data Right (CDR)

---

The Consumer Data Right (CDR) regulates the collection and handling of CDR data in line with privacy safeguards and rules that ensure users' data is managed securely and provide users with control over how their data is shared and used.

## 2. Accredited Data Recipients (ADRs)

---

An Accredited Data Recipient (ADR) is an organisation approved under the CDR framework to receive and manage consumer data securely. ADRs, such as Next Payments, are required to adhere to strict privacy and security rules, ensuring that consumer data is used only with their consent. We are committed to:

- Transparently disclosing how data is used.
- Ensuring secure transfer of consumer data.
- Implementing privacy safeguards to protect user consent.

*Note: As Next Payments performs name matching in real-time without storing PII, no consumer data is retained after processing.*

## 3. Key Benefits for Users

---

- **Choice and Control:** Users decide what data to share, how it's used, and who it can be disclosed to.
- **Manage Consent:** Users can view, modify, or revoke consents at any time.
- **Data Deletion Requests:** As no PII is stored, data deletion requests are not applicable; data is processed in real time and not retained.

## 4. Data Usage under CDR

---

Next Payments may use the data collected under the CDR framework for:

- **Personalised Services:** Tailoring recommendations to user activities during the session.
- **Operational Purposes:** Preventing fraud, detecting abuse, and generating analytical insights using de-identified data.
- **Communication:** Sending updates and notifications aligned with user preferences during the session.

The CDR data we request is the minimum necessary to fulfil these purposes, processed in real-time without storage to ensure privacy protection.

## 5. What is Consent?

---

Consent refers to the permission granted by a user to allow Next Payments to access, collect, and share their financial data with authorised third parties through our integration with Basiq's Open Banking platform. Consent ensures users maintain control over their data and are fully informed about how it is used.

## 6. Key Features of Consent Management

---

- **User-Initiated Consent:** Users provide explicit consent through the Next Payments app, ensuring they understand what data is being shared and with whom.
- **Granular Control:** Users can choose which accounts and data types (e.g., transactions, balances) they wish to share.
- **Time-Bound Consent:** Consent is session-based or time-limited, typically 48 hours, after which it expires unless renewed. As no PII is stored, data is processed in real time and not retained beyond the session.
- **Transparency:** Users receive clear information about the purpose of data sharing and the third parties involved.
- **Revocation Options:** Users can revoke consent at any time, stopping all data sharing immediately.

---

## 7. How Consent Works in the Next Payments App

---

Through our partnership with Basiq, Next Payments leverages Open Banking to securely connect to users' financial institutions. The consent process is seamless:

- **Initiation:** Users start the consent process within the Next Payments app when prompted to connect their bank account.
- **Authentication:** Users authenticate with their bank using secure credentials (e.g., via a redirect to their bank's login page).
- **Data Selection:** Users select which accounts and data types they wish to share.
- **Confirmation:** A summary of the consent agreement is displayed, including the purpose, duration, and third parties involved.
- **Completion:** Once confirmed, data is securely accessed and processed in real-time as per the user's preferences, with no PII stored.

## 8. Consent Management

---

When you give consent, you remain in control. You can easily manage your consent at any time—whether that means reviewing, updating, or withdrawing it—using any of the following methods:

- **Directly through the app:** This is the easiest and preferred method. Users can manage their consent directly in The Star app. Here, they can:
  - Navigate to manage funds.
  - Click manage CDR Consent at the bottom of the page.
  - Click Stop Sharing.
- **By contacting our support team via email:** Users can email [appsupport@nextpayments.com.au](mailto:appsupport@nextpayments.com.au) with the following details:
  - A clear description of the amendment or revocation request (e.g., "I wish to revoke consent for data sharing with [specific third party]" or "I wish to amend my consent to include only [specific account]"). For more details on managing consent, refer to our Consent Management Portal or the Basiq documentation at <https://api.basiq.io/docs/consent-actions>.

## 9. Data Retention, De-identification, and Consent Withdrawal

---

Next Payments does not store Personally Identifiable Information (PII). All data is processed in real-time during the user session and is not retained afterward. As a result, data retention, de-identification, and withdrawal of consent are inherently managed within our process. Users can revoke consent at any time, immediately halting all data processing, with no further action required for data deletion since no PII is stored.

---

 1300 659 918

 [info@nextpayments.com.au](mailto:info@nextpayments.com.au)

 [nextpayments.com.au](https://nextpayments.com.au)

---