

RAIN PRIVACY POLICY

Last updated: July 16, 2026

AT A GLANCE

- **Who we are:** “Rain” refers to Signify Holdings, Inc. and its affiliates, successors, assigns, and subsidiaries, including without limitation Nimbus LLC, doing business as Third National and Third National LLC, Rain Liquidity LLC, Rain Payments Services, Inc., and Rain Products, Inc. Rain is a financial technology provider. We are not a bank and do not hold deposits.
- **What we collect:** Identifiers (name, email), government IDs, financial/transaction data, and wallet addresses.
- **Why we collect it:** To provide services, verify your identity (KYC), prevent fraud, and comply with financial regulations.
- **Your choice:** You have rights to access, delete, or correct your data depending on where you live.
- **Blockchain:** Some data (wallet addresses, transaction amounts) is recorded permanently on public blockchains and cannot be deleted.

TABLE OF CONTENTS

1. [Scope and Applicability](#)
2. [Entity Roles and Data Flows](#)
3. [Personal Information We Collect](#)
4. [How and Why We Use Personal Information](#)
5. [Legal Bases for Processing](#)
6. [Biometric Information Notice](#)
7. [Blockchain, Stablecoin, and Digital Asset Disclosures](#)
8. [How We Share Personal Information](#)
9. [Financial Privacy Notice and GLBA](#)
10. [International Transfers](#)
11. [Retention](#)
12. [Security](#)
13. [Cookies, Tracking, Analytics, and Advertising](#)
14. [Automated Processing and Decision-Making](#)
15. [Your Privacy Rights](#)
16. [U.S. State Privacy Rights](#)
17. [EEA, UK, and Swiss Disclosures](#)
18. [Brazilian Resident Disclosures](#)

- 19. [Data Portability and Open Finance](#)
- 20. [Children's Privacy](#)
- 21. [Changes to This Privacy Policy](#)
- 22. [Contact Us](#)

23. **Scope and Applicability**

This Privacy Policy applies to the following products and services:

PRODUCT OR SERVICE	APPLICABLE ENTITY	SCOPE
Rain services	Signify Holdings, Inc. and its applicable operating subsidiaries	Rain's website, dashboards, partner-facing financial infrastructure, Rain Cards, card terms, authorized user services, stablecoin settlement services, and related services.
Avalanche Card services	Rain Liquidity LLC	Avalanche Card's website, mobile application, consumer Visa card services, wallet-based authentication, PIN recovery, digital asset collateral functionality, and related account services.
Third National services	Nimbus LLC, doing business as Third National and Third National LLC	Third National website, Visa card issuance, licensed lending, licensed money transmission, payment, settlement, and related services, as applicable.
European services	Rain Financial Services Europe Limited	European data processing and financial services where we determine the purposes and means of processing EU resident data.

This Privacy Policy does not apply to third-party websites, applications, or services that are governed by their own privacy notices.

When we provide services to business customers, fintech platforms, enterprises, or other partners, we may process personal information as a service provider or processor on behalf of that customer or partner. In those cases, the customer or partner may be responsible for its own privacy notice and for responding to privacy requests relating to personal information processed on its behalf.

When we process information directly for identity verification, fraud prevention, biometric verification, website analytics, account administration, regulated financial services, card issuance, customer support, or direct-to-consumer account services, the applicable Rain entity generally acts as a controller or business for that processing.

2. Entity Roles and Data Flows

Important Regulatory Disclaimer: Signify is a financial technology company. Signify and its affiliates (including Nimbus LLC, Rain Liquidity LLC, Rain Payments Services, Inc., and Rain Products, Inc.) are not banks, exchanges, or asset custodians. Rain does not provide FDIC insurance or hold deposits. Where applicable, banking and deposit services are provided by our respective regulated banking partners.

Signify provides financial technology, card, payment, stablecoin, and related services through different products and operating entities. The entity responsible for your information depends on the product you use and the purpose of processing.

Rain services: Rain provides financial infrastructure to businesses, fintechs, platforms, and enterprises. For partner-branded programs, Rain may process transaction history, card limits, account settings, usage data, and related information as a processor or service provider for the applicable partner. Rain may act as a controller or business for information it collects directly, including website interactions, support requests, identity verification, fraud prevention, biometric verification, security monitoring, and compliance activities.

Avalanche Card services: Avalanche Card is a consumer-facing Visa card service that may include wallet-based authentication, card services, consumer account management, digital asset collateral functionality, and related features. For Avalanche Card services, Rain Liquidity LLC generally acts as the controller or business for the personal information described in this Privacy Policy. When you use Avalanche Card services, we may collect wallet addresses, card transaction details, cryptocurrency collateral information, and on-chain transaction data associated with your wallet address.

Third National services: Nimbus LLC, doing business as Third National and Third National LLC, is a licensed lender, money transmitter and Visa-authorized card issuer that provides card issuance, payment, settlement, and related services. For card issuance and customer account services, Nimbus LLC generally acts as a controller. Nimbus LLC may share information with financial technology program managers, service providers, card networks, payment processors, or partners where necessary to provide card programs or services, subject to contractual restrictions and regulatory requirements.

How personal information flows between entities: We may share personal information among Rain entities and applicable partners where necessary to provide services, verify identity, issue

cards, process transactions, operate settlement services, support customer service, prevent fraud, conduct sanctions screening, comply with legal obligations, and maintain the security and integrity of our systems. Where Rain entities share personal information with each other, each entity may act as an independent controller, joint controller, processor, or service provider depending on the service, the agreement governing the processing, and the entity determining the purposes and means of processing.

3. Personal Information We Collect

We collect personal information directly from you, automatically through our services, from third parties, and through your use of our financial products and services.

Information you provide: We may collect information you provide when you create an account, apply for a card, request services, contact support, use our websites or applications, or otherwise interact with us. This may include:

CATEGORY	EXAMPLES
Identifiers and contact information	Name, email address, phone number, date of birth, residential address, shipping address, account credentials, and similar information.
Government identification information	Social Security number, driver's license information, passport information, government-issued identification numbers, and related verification information.
Financial and account information	Account balances, transaction history, payment history, financial data, repayment history where applicable, and related account information.
Business customer information	Company name, company address, formation documents, jurisdiction, tax identification number, registration number, beneficial ownership information, and wallet addresses, where applicable to Rain's B2B services.
Wallet and blockchain information	Wallet addresses, cryptocurrency type and amount used as collateral, on-chain transaction data, transaction metadata,

CATEGORY	EXAMPLES
	settlement activity, and wallet addresses associated with settlement activity.
Biometric information	Facial geometry or biometric identifiers derived from government identification documents and live images, where used for identity verification.
Communications	Support requests, correspondence, feedback, marketing preferences, and other communications with us.

Sensitive personal information: Certain information we collect may be considered sensitive personal information under applicable law, including government-issued identification numbers, financial account information, transaction history, authentication credentials, precise geolocation data, biometric information, and payment card data. We use sensitive personal information only as reasonably necessary to provide services, verify identity, prevent fraud, comply with legal and regulatory obligations, secure our services, and perform other purposes permitted by applicable law.

Information collected automatically: When you access our websites, applications, or digital services, we or our vendors may automatically collect information such as browser type, device type, operating system, device location signals, device identifiers, IP address, usage data, and information about interactions with our services. We may also collect information through cookies, pixels, software development kits, analytics tools, and similar technologies as described in the “Cookies, Tracking, Analytics, and Advertising” section below.

Transaction and account information: We collect transaction and account information when you use our services, including transaction amounts, transaction type, purchase details, timestamps, merchant information, card usage, account balances, repayment history where applicable, wallet addresses, and related transaction metadata.

Information from third parties: We may receive information from third parties, including credit bureaus, data providers, fraud detection services, identity verification providers, data analytics providers, banking partners, card networks, blockchain analytics providers, compliance monitoring providers, and other service providers.

4. How and Why We Use Personal Information

We use personal information for business, commercial, operational, and regulatory purposes, including to:

- Establish, maintain, and service accounts.
- Verify identity and perform KYC, AML, sanctions screening, customer identification, fraud detection, and onboarding.
- Assess eligibility for services, including card, account, payment, settlement, or related financial services.
- Underwrite and service credit, debit, prepaid, collateralized, or settlement products, as applicable.
- Process, authorize, settle, and monitor transactions.
- Support stablecoin, blockchain, card, and digital wallet functionality.
- Provide customer support and communicate with you about your account, services, security, notices, and policy updates.
- Send marketing communications where permitted by law and subject to your opt-out choices.
- Maintain, improve, and develop our services, products, websites, applications, security systems, fraud controls, and compliance processes.
- Conduct audits, enforce agreements, respond to legal process, and comply with contractual, legal, regulatory, accounting, tax, and reporting obligations.
- Protect the rights, safety, security, and integrity of Signify, our customers, partners, users, services, and the financial system.

5. Legal Bases for Processing

Where GDPR, UK GDPR, Swiss data protection law, LGPD, or similar laws apply, we process personal data only where we have a lawful basis.

LEGAL BASIS	HOW WE USE IT
Performance of a contract	To create accounts, provide services, issue payment cards, process transactions, provide settlement services, administer accounts, and take steps requested before entering into a contract.
Compliance with legal obligations	To comply with AML, BSA, sanctions, counter-terrorist financing, fraud monitoring, customer identification, regulatory reporting, recordkeeping, banking, tax, and other legal obligations.
Legitimate interests	To protect systems, prevent fraud, support operational resilience, improve services, conduct audits, defend legal claims, and manage security, provided those interests

LEGAL BASIS	HOW WE USE IT
	are not overridden by your rights and freedoms.
Consent	To process biometric information or send optional communications where consent is required by applicable law. You may withdraw consent, but some services may be unavailable without the relevant processing.
Legal claims	To establish, exercise, or defend legal claims.

1.

2. Biometric Information Notice

Where we use biometric verification, we may collect biometric identifiers, including facial geometry derived from your driver's license, passport, or other government identification and a live image you provide. We use biometric information to verify identity, prevent fraud, and comply with KYC, AML, and other regulatory requirements.

Biometric information may be collected and processed by a third-party identity verification service provider using encryption and other security safeguards. We do not sell biometric information.

We retain biometric information only as long as necessary for the purpose collected or within three (3) years of your last interaction with us, whichever occurs first, where required by applicable biometric privacy law. Biometric information may be retained for a longer period only where permitted or required by applicable law, including valid legal process, legal preservation obligations, or financial regulatory recordkeeping requirements.

Where consent is required, by proceeding with identity verification you consent to the collection, use, storage, and transmission of your biometric information as described in this Privacy Policy. You may withdraw consent by contacting us, but withdrawal may affect your ability to use our services. Where required by law, we will make our biometric retention and destruction policy available upon request.

7. Blockchain, Stablecoin, and Digital Asset Disclosures

Some Signify services support stablecoin, digital asset, wallet, or blockchain-enabled settlement features. Blockchain networks are distributed ledgers that are generally immutable, and

transaction details such as wallet addresses, timestamps, transaction amounts, and asset type (e.g., USDC, USDT, AVAX) may be recorded permanently on-chain.

We do not publish your legal name, residential address, Social Security number, or similar directly identifying information to public blockchains. We may delete, anonymize, or restrict personal information maintained in our internal systems where legally permissible, but we cannot alter or delete information recorded on public blockchain networks.

We may share wallet addresses and transaction data with blockchain analytics providers for sanctions compliance, fraud detection, risk monitoring, and transaction monitoring. Transfers involving stablecoins, digital assets, financial institutions, or virtual asset service providers may require us to collect and transmit information such as your name, address, and account identifier. Transactions involving self-custodial wallets may require additional verification of ownership.

Where a service supports self-custody integrations, Rain does not store or access your private keys or recovery seeds, and you are responsible for securing your credentials.

8. How We Share Personal Information

We share personal information only as permitted or required by law and consistent with our obligations as a financial services provider. We may share personal information with:

RECIPIENT CATEGORY	PURPOSE
Rain entities	To provide shared services, operate accounts, support products, manage fraud and compliance, and administer services.
Service providers, vendors, and advisors	Identity verification, fraud monitoring, payment processing, card network services, cloud infrastructure, compliance monitoring, analytics, security, customer support, and professional services.
Card networks and payment processors	Transaction processing, authorization, clearing, settlement, fraud prevention, and dispute support.
Banking partners and issuing banks	Account services, regulatory compliance, card issuance, settlement, transaction processing, and program administration.
Business customers and fintech partners	To provide partner-branded services, administer accounts, route privacy

RECIPIENT CATEGORY	PURPOSE
	requests, and support card or financial programs where Rain acts for a partner.
Merchants and businesses with whom you transact	To process, authorize, settle, verify, or support transactions.
Blockchain analytics providers	Sanctions screening, fraud monitoring, risk assessment, and compliance monitoring.
Regulators, law enforcement, courts, and governmental bodies	To comply with law, legal process, regulatory obligations, supervisory requests, or to protect legal rights.
Transaction counterparties and VASPs	To comply with transfer, payment, sanctions, anti-money laundering, travel rule, or similar obligations.
Corporate transaction parties	In connection with a merger, acquisition, financing, restructuring, due diligence process, asset sale, or similar corporate transaction.

Service providers are contractually required to use personal information only for authorized purposes and to maintain appropriate security measures. We may share aggregated, anonymized, or de-identified information where it cannot reasonably be linked to an identifiable person, subject to applicable law.

9. Financial Privacy Notice and GLBA

If you obtain financial products or services from us for personal, family, or household purposes, our separate [Financial Privacy Notice](#) describes how we, through our subsidiary Nimbus LLC, collect, share, and protect nonpublic personal information and your rights to limit certain types of sharing.

If there is a conflict between this Privacy Policy and an applicable Financial Privacy Notice for GLBA-covered information, the Financial Privacy Notice controls for GLBA-covered information. We may provide different Financial Privacy Notices depending on the product, entity, or program through which you receive financial products or services.

10. International Transfers

We may transfer, store, or process personal information in the United States and other jurisdictions where we, Rain entities, service providers, vendors, partners, or other recipients

operate. These jurisdictions may have data protection laws that differ from those in your country.

Where we transfer personal information from the EEA, UK, Switzerland, Brazil, or another jurisdiction that requires transfer safeguards, we use appropriate safeguards as required by applicable law, which may include European Commission Standard Contractual Clauses, the UK International Data Transfer Agreement or Addendum, ANPD-approved standard contractual clauses, adequacy decisions, transfer risk assessments, or other legally recognized transfer mechanisms.

11. Retention

We retain personal information for as long as necessary to provide services, comply with legal and regulatory obligations, resolve disputes, enforce agreements, prevent fraud, support audits, protect our rights, and maintain the safety, security, and integrity of our services and the financial system.

Retention periods vary depending on the type of information, when it was collected, whether it is needed to continue providing services, whether legal preservation obligations apply, and whether we must retain it for AML, KYC, banking, sanctions, tax, accounting, regulatory, or other compliance purposes. Customer identification records, transaction records, and related regulated financial services records may be retained for five years or longer following account closure where required by applicable law. For example, certain customer identification records may be retained for five years after an account is closed, or for credit card accounts, five years after the account is closed or becomes dormant, where required by applicable customer identification program rules.

Where biometric identifiers or biometric information are subject to a law requiring a shorter retention period, we retain and destroy that information in accordance with the shorter legally required period. For example, where the Illinois Biometric Information Privacy Act applies, biometric identifiers and biometric information are permanently destroyed when the initial purpose for collection has been satisfied or within three (3) years of the individual's last interaction with us, whichever occurs first, absent a valid warrant, subpoena, legal hold, or other applicable legal requirement.

Where retention is no longer required, we delete, anonymize, or de-identify personal information in accordance with our policies and applicable law.

12. Security

We maintain administrative, technical, and physical safeguards designed to protect personal information from unauthorized access, disclosure, alteration, or destruction. These safeguards may include encryption of sensitive data in transit and at rest, access controls, multifactor authentication, tokenization of sensitive payment data, transaction monitoring, internal security

testing, regular security assessments, employee training, and contractual safeguards for service providers.

Where applicable, our technology infrastructure supporting payment card data is designed to comply with PCI DSS requirements, and Rain maintains SOC 2 Type II certification.

No method of transmission or storage is completely secure. You are responsible for protecting passwords, wallet credentials, private keys, recovery phrases, PINs, and other account access credentials where applicable.

13. Cookies, Tracking, Analytics, and Advertising

We may use cookies, pixels, software development kits, session cookies, security cookies, analytics tools, advertising technologies, and similar technologies to operate our services, recognize users, remember preferences, improve functionality, measure performance, analyze trends, prevent fraud, and deliver content or advertisements.

You can configure your browser to refuse cookies or notify you when cookies are being sent, but some features may not work properly without cookies. Certain analytics, advertising, and related third parties may process information under their own privacy notices.

Our websites do not currently respond to Do Not Track browser signals. We honor Global Privacy Control signals as required by applicable law, including as a request to opt out of sale, sharing, targeted advertising, or similar processing where applicable.

14. Automated Processing and Decision-Making

We may use automated systems to support fraud detection, sanctions screening, transaction monitoring, identity verification, biometric matching, eligibility assessments, and risk management.

Where automated processing produces legal or similarly significant effects and applicable law grants you rights, you may request information about the processing, request human review, express your point of view, and contest the decision, subject to legal and regulatory limitations.

15. Your Privacy Rights

Depending on your location, relationship with us, and the type of information involved, you may have rights to access, correct, delete, port, restrict, or object to processing of your personal information, to withdraw consent, to opt out of certain sharing or targeted advertising, to limit certain uses of sensitive personal information, and to appeal certain decisions.

These rights may be limited where processing is necessary to provide services, comply with legal obligations, satisfy financial regulatory requirements, prevent fraud, complete transactions,

maintain security, preserve evidence, or establish, exercise, or defend legal claims.

How to exercise rights: You may submit privacy requests using the contact information in Section 22. If your request relates to a partner-branded product where Rain acts as processor or service provider, we may refer the request to the applicable partner or work with the partner to respond. If your request relates to information controlled directly by Rain, including without limitation Nimbus LLC, Rain Liquidity LLC, Rain Payments Services, Inc., and Rain Products, Inc., the applicable Rain entity will respond in accordance with applicable law. We may verify your identity before processing a request. You may authorize an agent to submit a request where permitted by law, subject to verification and authorization requirements.

16. U.S. State Privacy Rights

Residents of certain U.S. states may have rights to request access, correction, deletion, portability, or information about categories of personal information collected, used, disclosed, sold, or shared. They may also have rights to opt out of sale, sharing, targeted advertising, or certain profiling, and to limit certain uses of sensitive personal information.

Because some Rain entities provide financial products or services subject to GLBA, certain personal information collected in connection with those products or services may be exempt from some state privacy law requirements.

We do not sell sensitive personal information such as biometric data or precise geolocation where prohibited by applicable law (such as under the Maryland MODPA and similar state privacy frameworks). California residents may request information once per calendar year about categories of personal information disclosed to third parties for their direct marketing purposes, if any. We honor Global Privacy Control signals where required by applicable law.

17. EEA, UK, and Swiss Disclosures

For individuals located in the European Economic Area (EEA), the United Kingdom (UK), or Switzerland, we process personal data in accordance with applicable data protection laws, including the GDPR, UK GDPR, and Swiss data protection law.

The applicable controller depends on the product, service, and processing purpose. For the majority of our B2B Services, Signify Holdings, Inc. acts as a Data Processor on behalf of our Partners. For information collected directly from you (like identity verification, fraud prevention, and biometric data collection), Rain acts as a Data Controller.

Subject to applicable limitations and our role in processing your data, you may have the right to:

- Request access to your personal data.
- Request rectification of inaccurate or incomplete data.

- Request erasure of your personal data.
- Restrict the processing of your data.
- Request data portability.
- Object to processing based on legitimate interests.
- Lodge a complaint with a supervisory authority in your country of residence, place of work, or where an alleged infringement occurred.

You may also have rights relating to automated decision-making that produces legal or similarly significant effects. If required by applicable law, the relevant Rain entity will appoint an EU or UK representative and make contact details available. For EU, UK, and Swiss data protection inquiries, you may contact us at dpo@rain.xyz or the other representative contact published by the relevant Rain entity.

As noted in the European services section above, Rain Financial Services Europe Limited is Rain's EU representative for purposes of applicable EU data protection laws and may be contacted about EU data protection inquiries using the contact information provided in this Privacy Policy.

18. Brazilian Resident Disclosures

If you are a resident of Brazil, you may have specific rights under the Lei Geral de Proteção de Dados (LGPD).

Our Role: For information processed at the direction of our Partners, we act as a "Processor" and the Partner is the "Controller" responsible for fulfilling your rights. We act as a "Controller" for direct identity verification and biometric data.

Subject to applicable exceptions, you have the right to:

- Confirm the existence of processing activities.
- Access your personal data.
- Correct incomplete, inaccurate, or out-of-date data.
- Anonymize, block, or delete unnecessary or excessive data, or data processed in noncompliance with the LGPD.
- Request portability of your data to another service or product provider.
- Obtain information about the public and private entities with which we have shared your data.
- Withdraw your consent, and request deletion of data processed based on your consent.

For partner-controlled data, the relevant partner may be responsible for responding to requests. For Signify-controlled data, contact us using the contact information below. Transfers from Brazil to the U.S. are protected by ANPD-approved Standard Contractual Clauses.

DPO in Brazil: For purposes of Brazilian data protection law, Rain has appointed Barcellos Tucunduva Advogados as its data protection officer (Encarregado pelo tratamento de dados pessoais). You may contact Dr. Luiz Fernando Andrade at privacidade@btlaw.com.br or +55 (11) 3069 9080.

19. Data Portability and Open Finance

Where available and required by law, we support your ability to access and move your financial data in compliance with Open Finance mandates. We do not use screen scraping to collect login credentials. Where you authorize a third party to access account data, we share only data reasonably necessary for the requested service through secure methods, such as APIs where available.

20. Children's Privacy

Our services are not directed to individuals under 18 years of age. We do not knowingly collect, accept, request, or solicit personal information from children, nor do we knowingly market to children. If we receive knowledge of anyone under the age of 13 who has provided personal information to us, we will take steps to delete that information from our Services.

21. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. For material changes that affect how we use personal information, we will provide notice in accordance with applicable law, which may include notice by email, prominent notice on our website, or other appropriate means at least 30 days before they take effect.

22. Contact Us

For questions about this Privacy Policy or to exercise privacy rights, contact the applicable Rain entity:

ENTITY OR SERVICE	CONTACT
Rain services	privacy@rain.xyz
Avalanche Card	support@avalanchecard.com
Third National services	legal@rain.xyz
EU/UK data protection inquiries	dpo@rain.xyz
Brazil DPO	Barcellos Tucunduva Advogados, Dr. Luiz Fernando

ENTITY OR SERVICE	CONTACT
	Andrade, privacidade@btlaw.com.br , +55 (11) 3069 9080

Change Log

Date	Changes Made	Approver
May 13, 2026	Initial policy consolidation	Legal Department
July 11, 2026	Corrections to entity names, fictitious business names, and email hyperlinks; definition of Rain; change of biometric data retention period from 5 to 3 years; addition of licensed money transmission services in scope of Third National services; identification of Rain's EU data protection representative; formatting changes	Legal Department
July 11, 2026	Minor language change to Applicable Entity for Rain services; removal of bill page from Scope of Rain services	Legal Department