

BITPAY, INC.

Applicant Privacy Notice

Effective Date: August 1, 2026

This Notice applies exclusively to job applicants, candidates, and individuals participating in BitPay's recruitment and hiring process.

For information about how BitPay handles consumer data, please review the BitPay Privacy Notice at bitpay.com/about/privacy.

SCOPE AND APPLICABILITY

This Applicant Privacy Notice (“**Notice**”) explains how BitPay, Inc. (“**BitPay**,” “**we**,” “**us**,” or “**our**”) collects, uses, retains, discloses, and protects the Personal Information of individuals who:

- Apply for employment or contract positions with BitPay;
- Submit résumés or expressions of interest through any channel;
- Participate in screening, assessments, or interviews; or
- Are contacted by or on behalf of BitPay in connection with a potential role.

This Notice supplements and does not replace any jurisdiction-specific disclosures provided separately. Where applicable law requires specific additional disclosures, those are set forth in the [U.S. State Disclosures](#) section of this Notice and the [International Disclosures](#) section of this Notice.

PERSONAL INFORMATION WE COLLECT

The categories of Personal Information we collect, and illustrative examples of each, are described below. Collection is limited to information that is relevant to the recruitment purpose and permitted under applicable law.

A. Core Identifiers and Contact Information

- Full legal name, preferred name, pronouns (where voluntarily provided)
- Email address, telephone number, mailing address
- Professional profiles (e.g., LinkedIn URL) or personal websites provided by the applicant
- Government-issued identification numbers, where required for eligibility verification

B. Professional and Educational Background

- Résumé, curriculum vitae, cover letter, and application materials
 - Work history, titles held, employment dates, and names of prior employers
 - Educational credentials, degrees, certifications, and transcripts
-

- Professional licenses, registrations, and memberships
- References and reference check responses

C. Application and Assessment Data

- Written responses to application questions
- Interview notes, scores, and evaluations
- Skills assessments, coding exercises, or case study outputs
- Compensation expectations, availability, and geographic preferences
- Offer and negotiation correspondence

D. Sensitive Personal Information (where lawfully required)

BitPay collects the following sensitive categories only where required by law, for legally mandated compliance programs (including AML/KYC obligations applicable to certain roles), or with your explicit consent. Collection is limited to the minimum necessary.

- Government-issued identifiers (e.g., passport number, national ID, driver's license number, Social Security Number) — for background verification or work authorization
- Criminal history — where permitted by applicable state or country law and relevant to the position
- Financial background or sanctions screening data — for roles with fiduciary or regulatory requirements under FinCEN, BSA, or equivalent regulations
- Disability and accommodation information — provided voluntarily to support an interactive accommodation process
- Diversity and inclusion data (race, ethnicity, gender, veteran status) — collected voluntarily and used only in the aggregate for EEO reporting and DEI program evaluation

E. Device, Technical, and Usage Data

- IP address, browser type, device identifiers, and operating system information
- Pages visited on the careers site, session timestamps, and referral source
- Cookies and similar tracking technologies

F. Audio, Visual, and Communications Data

- Interview recordings (video or audio) where notice is provided and permitted by law
- Electronic correspondence between you and BitPay or its authorized recruiters

G. Inferences and Evaluations

- Suitability assessments and role-fit determinations derived from application materials
 - Notes and scores generated during structured interview processes
-

HOW WE COLLECT PERSONAL INFORMATION

Provision of Personal Information. Providing Personal Information for the recruitment process is generally voluntary. However, failure to provide certain information (such as work authorization documentation or required identification) may limit our ability to evaluate your application or comply with legal obligations.

We collect Personal Information through the following channels:

Source	Examples
Directly from you	Application forms, résumé submissions, cover letters, interview responses, assessment submissions, correspondence.
Automatically from your device	Careers site cookies, log files, analytics tools (see BitPay’s Privacy Notice and BitPay’s Cookie Notice for more information on how BitPay processes this information)
Third-party recruiters and staffing agencies	Résumé submissions, candidate profiles forwarded on your behalf
Professional networking platforms	Public LinkedIn profiles or other professional profiles you have made publicly available
References	Information provided by individuals you have designated as professional references
Background and verification providers	Third-party services used to conduct pre-employment background checks, employment verification, and credential checks, where authorized
Government and public records	Sanctions lists, regulatory databases, and public filings for applicable regulatory compliance roles
ATS and HR systems	Applicant tracking systems and HR information systems used to manage the recruitment process

HOW WE USE PERSONAL INFORMATION

We use Personal Information collected in the recruitment process for the following purposes:

A. Primary Recruitment Purposes

- Evaluating your qualifications, skills, and suitability for specific roles
- Communicating with you throughout the application and hiring process
- Scheduling and conducting interviews and assessments
- Verifying identity, employment history, educational credentials, and work authorization
- Conducting background checks where permitted or required by law
- Making hiring decisions
- Preparing employment offer documentation
- Supporting onboarding processes if an offer of employment is accepted

B. Legal and Regulatory Compliance Purposes

As a regulated financial institution and cryptocurrency payment processor, BitPay is subject to the Bank Secrecy Act (BSA), FinCEN regulations, OFAC sanctions requirements, and state money transmitter licensing laws. For certain roles, we are legally required to screen candidates against government sanctions lists and conduct enhanced due diligence. Processing for these purposes constitutes a legal obligation.

- Complying with applicable employment, labor, immigration, and tax laws
- Meeting anti-money laundering (AML), know-your-employee (KYE), and sanctions screening obligations for applicable roles
- Maintaining legally required employment records and audit trails
- Establishing, exercising, or defending legal claims
- Responding to lawful governmental or regulatory requests

C. Legitimate Business Interests

- Improving and optimizing BitPay’s recruitment processes and candidate experience
- Supporting diversity, equity, and inclusion initiatives (using aggregate, de-identified data only)
- Detecting and preventing fraudulent applications or misrepresentation
- Protecting the security and integrity of BitPay’s systems and workforce
- Maintaining talent pools of qualified candidates for future opportunities (where consent is obtained or otherwise permitted)

D. Lawful Bases (EU/UK Applicants). Where the GDPR or UK GDPR applies, we rely on the following legal bases:

Legal Basis	Processing Activity
Steps to enter into a contract (Art. 6(1)(b))	Core recruitment activities: evaluating your application, conducting interviews, making hiring decisions
Legal obligation (Art. 6(1)(c))	Sanctions screening, AML/KYE compliance, employment authorization verification, record-keeping
Legitimate interests (Art. 6(1)(f))	Fraud prevention, system security, process improvement, talent pipeline maintenance
Consent (Art. 6(1)(a) / Art. 9(2)(a))	Voluntary diversity data collection; retention of your application for future opportunities; any non-mandatory sensitive data processing

E. Combining Personal Information. We may combine Personal Information collected from different sources described in this Notice, including information collected directly from you, automatically, and from third parties, to support the purposes described above, including improving recruitment processes, verifying information, and ensuring compliance with applicable legal obligations.

F. De-Identified Information. We or our service providers may de-identify or aggregate Personal Information so that it can no longer reasonably be used to identify you. Where we de-identify information, we will maintain and use

such information in de-identified form and will not attempt to re-identify it, except as permitted by applicable law. We require service providers that receive de-identified information to comply with similar obligations.

DISCLOSURE OF PERSONAL INFORMATION

We disclose applicant Personal Information only as described below:

Recipient Category	Purpose / Basis for Disclosure
Applicant Tracking System (ATS) and HRIS providers	Core recruitment platform hosting and applicant data management
Background check and identity verification providers	Employment and credential verification; criminal history checks (where permitted); sanctions screening
Interview scheduling and video conferencing platforms	Facilitating remote and in-person interview processes
Compensation and payroll system vendors (pre-hire)	Offer letter generation and onboarding preparation
BitPay affiliates and parent/subsidiary entities	Collaborative hiring for shared or affiliated roles; global HR coordination
Regulators, law enforcement, and government agencies	Responding to lawful legal process; AML/sanctions compliance reporting; immigration authorities for work authorization
Professional references	Employment verification (only with your prior designation)
Transaction counterparties	In the event of a merger, acquisition, reorganization, or sale of assets, applicant data may be transferred as part of that transaction
Legal advisors and auditors	Exercising or defending legal claims; regulatory compliance audits

These recipients act as either service providers (processors) acting on our behalf or independent controllers where required by law. We enter into data processing agreements or other appropriate contractual arrangements with all third-party service providers who process Personal Information on our behalf, requiring them to implement appropriate security measures and to use the data only for authorized purposes.

We do not sell applicant Personal Information. We also do not share applicant Personal Information for cross-context behavioral advertising, except for limited cookie-based activities on our careers site as described in the [Cookies and Tracking Technologies](#) section of this Notice.

AUTOMATED PROCESSING AND AI-ASSISTED TOOLS

BitPay does not make hiring decisions based solely on automated processing. Automated tools may be used to support elements of the recruitment process; however, all decisions that have a legal or similarly significant effect involve meaningful human review.

Where applicable under law, you may have the right to request information about the use of automated processing, including meaningful information about the logic involved and the potential consequences of such processing, as well as the right to request human review and submit observations.

COOKIES AND TRACKING TECHNOLOGIES

BitPay’s careers site uses cookies and similar tracking technologies to support site functionality, analyze usage, and, in limited circumstances, deliver relevant content. Applicants are encouraged to review the [BitPay Cookie Policy](#) and the [BitPay Privacy Notice](#) for detailed information about the categories of cookies used, the parties involved, and how to manage your preferences.

BitPay honors Global Privacy Control (GPC) signals. If your browser transmits a GPC signal, BitPay will treat it as a valid opt-out of the sale and sharing of Personal Information for targeted advertising purposes, consistent with applicable state law.

THIRD-PARTY WEBSITES AND SERVICES

Our careers site and recruitment process may contain links to third-party websites, platforms, or services that are not owned or controlled by BitPay (such as LinkedIn or external application platforms). This Notice does not apply to those third parties. We are not responsible for the privacy, security, or data handling practices of third-party websites or services. We encourage you to review the privacy notices of any third party before providing your Personal Information.

HOW LONG WE KEEP PERSONAL INFORMATION

Retention periods are determined based on the duration of the recruitment process, applicable legal requirements, regulatory obligations, and BitPay’s legitimate business needs. We retain applicant Personal Information for the periods described below, or as otherwise required or permitted by law.

Applicant Status	Retention Period
Unsuccessful applicants (general)	Up to 3 years from the date of the final decision, unless a shorter or longer period is required by applicable law
Unsuccessful applicants (ADA/EEOC record-keeping)	Minimum of 1 year from the date of the personnel action (2 years for employers with 150+ employees or federal contractors)
Hired employees	Data is incorporated into the employee record and retained per BitPay’s Employee Data Retention Policy
Background check records	As required under the Fair Credit Reporting Act (FCRA) and applicable state equivalents
AML/KYE screening records (applicable roles)	Minimum of 5 years from the date of collection, consistent with BSA/FinCEN requirements
Talent pool / future opportunity consent	Until consent is withdrawn or up to 3 years from initial collection, whichever is earlier

Following the applicable retention period, we will securely delete or anonymize applicant Personal Information, unless an exception applies (e.g., an active legal claim, regulatory inquiry, or ongoing litigation hold).

INTERNATIONAL DATA TRANSFERS

BitPay, Inc. is headquartered in Atlanta, Georgia, United States. Personal Information collected through the recruitment process may be transferred to, stored in, and processed in the United States and in other countries where BitPay’s affiliates, service providers, or partners are located.

Where applicable law requires legal mechanisms for cross-border data transfers, we rely on the following safeguards:

Transfer Mechanism	Applicable Jurisdiction
Standard Contractual Clauses (SCCs) approved by the European Commission	EEA/EU to third countries
UK International Data Transfer Agreement (IDTA) or UK Addendum to EU SCCs	UK to third countries
Contractual protections and vendor data processing agreements	Canada (PIPEDA/Law 25), Brazil (LGPD), and other applicable jurisdictions
Privacy assessments / Transfer Impact Assessments (TIAs)	Conducted where required under applicable data protection law

SECURITY

BitPay implements and maintains administrative, technical, and physical safeguards designed to protect applicant Personal Information from unauthorized access, use, disclosure, alteration, or destruction. No transmission of data over the Internet or storage system can be guaranteed to be 100% secure. If you believe that your Personal Information may have been compromised, please contact us immediately at dpo@bitpay.com.

YOUR PRIVACY RIGHTS

Depending on your location, you may have certain rights with respect to your Personal Information. The table below provides a global overview; jurisdiction-specific rights are detailed in the [U.S. State-Specific Disclosures](#) section of this Notice and the [International Disclosures](#) section of this Notice.

Right	Description
Access / Know	Request information about the Personal Information we hold about you and how it is processed
Correction / Rectification	Request that we correct inaccurate or incomplete Personal Information
Deletion / Erasure	Request that we delete your Personal Information (subject to applicable legal exceptions)
Restriction of Processing	Request that we restrict the processing of your Personal Information in certain circumstances
Data Portability	Receive a copy of certain Personal Information in a structured, machine-readable format
Objection	Object to certain processing activities, including processing based on legitimate interests
Opt-Out (U.S. State Laws)	Opt out of the sale, sharing, or use of Personal Information for targeted advertising
Automated Decision-Making	Request human review or contest decisions made by automated means (see the Automated Processing and AI-Assisted Tools section of this Notice)
Withdraw Consent	Where processing is based on your consent, withdraw that consent at any time
Appeal	Appeal a decision regarding your rights request (available in certain U.S. states)
Complaint to Regulator	Lodge a complaint with the applicable supervisory authority or data protection authority

How to Exercise Your Rights:

[DSR Portal](#)

Email: dpo@bitpay.com

Toll-Free: +1 (888) 914-9661

We will respond within the timeframe required by applicable law. We may verify your identity before processing your request. You will not be discriminated against for exercising your privacy rights.

U.S. State-Specific Disclosures

California (CCPA/CPRA) — Notice at Collection

This section serves as BitPay's Notice at Collection for California residents under the California Consumer Privacy Act, as amended by the California Privacy Rights Act (CCPA/CPRA) and applies at or before the point of collection of Personal Information. It is incorporated by reference into the main body of this Notice.

Categories of Personal Information Collected (CA Residents): See the [Personal Information We Collect](#) section of this Notice for more information about the categories of Personal Information we collect.

Categories include:

- ⇒ Identifiers
- ⇒ California Customer Records information
- ⇒ Professional/Employment Information; Education Information
- ⇒ Sensitive Personal Information (as defined by CPRA)—*we do not use Sensitive Personal Information to infer characteristics about applicants*
- ⇒ Internet or Network Activity
- ⇒ Audio/Visual Information
- ⇒ Inferences

Purposes for Collection: See the [How We Use Personal Information](#) section of this Notice for more information about how we collect Personal Information.

Primary business purposes include:

- ⇒ recruitment and hiring
- ⇒ legal compliance
- ⇒ legitimate business operations

Categories of Recipients: See the [Disclosure of Personal Information](#) section of this Notice for more information on how we disclose Personal Information.

We do not sell applicant Personal Information. We also do not share applicant Personal Information for cross-context behavioral advertising purposes, except for limited use of cookies and similar technologies as described in the [Cookies and Tracking Technologies](#) section of this Notice.

Retention: See the [How Long We Keep Personal Information](#) section of this Notice for more information on how long we retain Personal Information. Retention periods are calibrated to the purpose of collection and applicable legal requirements.

Your California Rights. California residents have the following rights with respect to Personal Information that is not exempt under the CCPA's Gramm-Leach-Bliley Act (GLBA) carve-out (which applies to certain financial services data):

- **Right to Know / Access:** Request the categories and specific pieces of personal information collected about you
- **Right to Delete:** Request deletion of Personal Information (subject to exceptions)
- **Right to Correct:** Request correction of inaccurate personal information
- **Right to Opt-Out of Sale or Sharing:** We do not sell applicant personal information; limited cookie-based sharing may occur on the careers site (see the [Cookies and Tracking Technologies](#) section of this Notice)
- **Right to Limit Use of Sensitive Personal Information:** We use SPI only as necessary for recruitment, legal compliance, and security — no additional limitation is currently required
- **Right to Non-Discrimination:** You will not be discriminated against for exercising your CCPA rights

How to exercise California rights. [DSR Portal](#) | Email: dpo@bitpay.com | Phone: +1 (888) 914-9661 (PIN: 910 593)

Authorized Agents: You may designate an authorized agent to submit a request on your behalf. We may require the agent to provide written authorization signed by you, and we may also require you to verify your identity directly with us or confirm that you provided the agent permission to submit the request.

Verification: To protect your privacy, we will verify your identity before processing your request. The level of verification required will depend on the sensitivity of the information and the nature of your request. This may include matching information you provide with information we maintain in our records or requesting additional information where necessary.

Other States

Certain U.S. state privacy laws provide consumer privacy rights; however, these laws generally do not apply to Personal Information collected in the employment or applicant context, including information collected as part of BitPay's recruitment process. Notwithstanding the above, BitPay may, in its discretion and where operationally feasible, extend certain rights to applicants consistent with its broader privacy practices.

International Disclosures

Brazil (Lei Geral de Proteção de Dados — LGPD)

This section applies to applicants located in Brazil and reflects obligations under the Lei Geral de Proteção de Dados Pessoais (LGPD), Law No. 13,709/2018. BitPay processes personal data of Brazilian applicants on the legal bases of: (i) compliance

with a legal or regulatory obligation; (ii) execution of a contract or pre-contractual measures; and (iii) legitimate interest, where applicable and balanced against applicant rights.

Your LGPD Rights (Art. 18)

- Confirm whether your personal data is being processed
- Access your personal data
- Correct incomplete, inaccurate, or outdated personal data
- Anonymize, block, or delete unnecessary or excessive personal data
- Data portability to another service provider
- Information about the public and private entities with which BitPay has shared your data
- Information about the possibility of denying consent and the consequences of doing so
- Revoke consent at any time

To exercise your LGPD rights, contact us at legal@bitpay.com. Requests will be addressed within 15 business days, consistent with applicable ANPD guidance.

Canada (PIPEDA and Provincial Privacy Laws)

This section applies to applicants located in Canada and supplements the main body of this Notice to reflect obligations under the Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial privacy laws (including Québec's Law 25 / Bill 64).

Collection, use, and disclosure of Personal Information about Canadian applicants is based on consent (express or implied, depending on the sensitivity of the information and the context of collection) or as otherwise permitted by applicable law.

Your Canadian Privacy Rights

- Right of access — request access to Personal Information we hold about you and information about how it has been or may be used or disclosed
- Right to correction — request correction of Personal Information that is inaccurate or incomplete
- Right to withdraw consent — withdraw consent to the processing of your Personal Information at any time, subject to legal or contractual restrictions and reasonable notice
- Right to information about cross-border transfers — request information about the safeguards in place when Personal Information is transferred outside Canada

To exercise your rights, contact BitPay's Privacy Officer at legal@bitpay.com or via the DSR Portal. We respond to requests within 30 days (extendable by a further 30 days where necessary, with notice).

Québec Note: If you are a Québec resident, you may have additional rights under Law 25, including the right to data portability and the right to be informed of cross-border transfers. BitPay conducts Privacy Impact Assessments (PIAs) as required before transferring Personal Information outside Québec. Where applicable, you will be informed if a decision is based exclusively on automated processing and provided with an opportunity to submit observations.

European Union and United Kingdom (GDPR / UK GDPR)

This section applies to applicants located in the European Economic Area (EEA), European Union (EU), or United Kingdom (UK) and supplements the main body of this Notice. In the event of any conflict between this section and the main body, this section prevails for EU/UK applicants.

BitPay, Inc. (Atlanta, GA) is the data controller for applicant personal data collected from EU and UK residents. Applicants in the EU/UK may contact legal@bitpay.com with any GDPR-related queries.

Your GDPR / UK GDPR Rights

- Right of access (Art. 15) — obtain a copy of personal data we hold about you
- Right to rectification (Art. 16) — correct inaccurate personal data
- Right to erasure (Art. 17) — request deletion (“right to be forgotten”), subject to exceptions
- Right to restrict processing (Art. 18) — request temporary limitation of processing
- Right to data portability (Art. 20) — receive personal data in a structured, machine-readable format
- Right to object (Art. 21) — object to processing based on legitimate interests
- Rights in relation to automated decision-making (Art. 22) — not to be subject to solely automated decisions with significant effects
- Right to withdraw consent — where processing is consent-based, withdraw at any time without affecting prior lawful processing

Complaints. You may also lodge a complaint with the competent supervisory authority in your country. We encourage you to contact us first so that we may address your concern directly.

Data Protection Officer. You may contact BitPay’s Data Protection Officer at dpo@bitpay.com if you have any questions about this Notice.

Special Categories of Personal Data. Where BitPay processes special category data (Art. 9 GDPR) — including diversity monitoring data or disability/accommodation information — we rely on explicit consent (Art. 9(2)(a)) or, where applicable, processing necessary for obligations and rights in the field of employment law (Art. 9(2)(b)). Provision of special category data is voluntary except where required by law.

SMS / TEXT MESSAGE TERMS

By providing your mobile phone number and consenting to receive text messages from BitPay in connection with the recruitment process, you agree to the following:

- You consent to receive recruitment-related text messages (e.g., interview confirmations, scheduling links, status updates) to the mobile number you have provided
- Message and data rates may apply depending on your mobile carrier and plan
- Message frequency varies and is limited to the recruitment process
- To opt out of SMS messages at any time, reply STOP to any text message from BitPay
- For assistance, reply HELP or contact us at dpo@bitpay.com
- BitPay does not use SMS messaging for marketing or promotional purposes in connection with the applicant notice
- Your consent to SMS is not a condition of applying for or being considered for employment

CHANGES TO THIS NOTICE

BitPay reserves the right to update or amend this Notice at any time. When we make material changes, we will provide notice through the careers site or by direct communication where required by applicable law. The effective date at the top of this Notice indicates when it was last revised. We encourage you to review this Notice periodically.

HOW TO CONTACT US

If you have questions about this Notice, wish to exercise your privacy rights, or have a concern about our data practices, please contact us:

Channel	Contact Information
Privacy Officer / DPO	dpo@bitpay.com
DSR Portal	https://privacyportal-eu-cdn.onetrust.com/dsarwebform/c44272b8-1e9d-4ff3-840c-4af3bbc9ce8e/44b3f45f-9154-4e50-9561-2907b5bb3da7.html
Toll-Free Hotline	+1 (888) 914-9661 (PIN: 910 593) — California rights requests
Mail	BitPay, Inc., Attn: Legal / Privacy, 1870 The Exchange SE, Ste 220, PMB 91017, Atlanta, GA 30339