Privacy and Data Security Policy

October 16, 2025

Purpose

This privacy and data security policy (this "***Policy***") defines the commitment of Burford Capital Limited and its subsidiaries ("***Burford***") to the protection and preservation of the privacy of each individual or organization whose information it holds. It also sets forth the steps Burford has taken to secure the data relating to the individuals or organizations that it may collect.

Scope

This Policy explains how Burford collects, stores and uses Personal Data (as defined below) across its business. It applies to all of Burford's affiliates and business operations around the world.

Collection, use and disclosure of Personal Data

To allow us to provide and offer our products and services, we collect and use data and disclose data to third parties. Burford is firmly committed to protecting the privacy and the confidentiality of each individual or organization whose information it holds.

In this Policy, "***Personal Data***" refers to data that could be used, alone or in combination with other data, to identify individuals. We may collect and use the following types of Personal Data:

- names and contact information, including email address, telephone number, address and company details;
- information to check and verify an individual's identity, e.g., date of birth, copies of IDs and proof of address;
- gender;
- location data;
- financial information, including account details, national insurance number, tax details, billing information and transaction and payment card information;
- professional online presence, e.g., LinkedIn profile and information on the UK Companies House (and equivalent company registries);
- information to enable us to undertake credit or other financial checks, including source of funds; and
- information on use of our website, information technology, communication and other systems.

We collect and use this Personal Data to provide our products and services.

Disclosure or use of Personal Data

We are strongly committed to privacy and confidentiality and we will not exchange or sell Personal Data without consent outside of Burford, except if it is already in the public domain, in connection with a legal or regulatory obligation or otherwise in accordance with this Policy.

Agents and service providers

Occasionally, we contract with other companies and individuals to perform functions or services on our behalf, such as hosting our website, performing administration services in respect of Burford, sending email messages, making phone calls on our behalf or otherwise gathering and processing Personal Data as may be required for Burford's legitimate interests, including in respect of any legal proceedings. They may have access to Personal Data, such as addresses, needed to perform their functions, but are restricted from using it for purposes other than providing services for Burford and will be subject to specific contractual requirements in relation to the processing of such Personal Data.

Business transfers

As we continue to develop our business, we might sell or buy assets or businesses. In such transactions, user information generally is one of the transferred business assets. Also, if either a Burford entity itself or substantially all of a Burford's entity's assets were acquired, Personal Data may be one of the transferred assets. We may also disclose information as we deem necessary to satisfy any applicable law, regulation, legal process or governmental request.

Investors and their affiliates

Burford mainly gathers Personal Data concerning investors in Burford and persons affiliated with them through the following sources:

- Subscription forms, investor questionnaires and other information provided by the investor (including identification and verification documentation) in person, by telephone (which may be recorded), electronically or by any other means. This information includes identifiers, such as names, addresses, nationalities, tax identification numbers, financial and investment qualifications, and may include special category data, such as information regarding criminal convictions.
- Transactions, including account balances, investments, distributions, payments and withdrawals.

We may use Personal Data that we hold to send periodic updates about Burford's business, activities or opportunities, in particular, by email or mail/post. We will ensure that the option to opt-out is easily accessible.

Keeping Personal Data secure

We have appropriate security measures to prevent Personal Data from being accidentally lost, used or accessed unlawfully. We limit access to Personal Data to those who have a genuine business need to access it. We also have a Written Information Security Program in place should Burford experience a suspected data security breach. We will notify any impacted party and any applicable regulator of a suspected data security breach where we are legally required to do so.

Personal Data collected may be processed and stored anywhere in the world by Burford and its technology service providers. By providing information to Burford, individuals and organizations

provide their consent to the transfer of the information into or through any jurisdiction for processing in accordance with this Policy. We endeavor to maintain appropriate safeguards commensurate with the sensitivity of the Personal Data we collect, use and maintain. However, as effective as our security measures may be, no security system is impenetrable. We cannot guarantee the security of our database, nor can we guarantee that information supplied will not be intercepted while being transmitted to us over the Internet or otherwise.

How long Personal Data will be kept

Subject to applicable law, we will take reasonable measures not to keep Personal Data for longer than we need it for the purpose for which it is used.

Different retention periods apply to different types of Personal Data.

Further information on Burford's privacy practices, including how we will handle information voluntarily provided to us, how and why we use Personal Data, website and cookies, discussion forum and chat room use, international transfers of Personal Data, disclosure of Personal Data, information related to employment, minors and marketing and your rights, is available in our privacy policies for the United States and the United Kingdom / European Union. These privacy policies apply across all Burford's affiliates around the world.

Our detailed US privacy policy measures can be found here.

Our detailed UK and European Union privacy policy measures can be found here.

Data security

Our business relies heavily on data security and the use of electronic devices, computer networks and the Internet. Since our inception in 2009, we have been hypersensitive to securing our data and have operated on an entirely cloud-based platform. Our data does not sit on our own servers, but rather on the servers of world-class technology companies, whose data protection and security are vetted by our information technology team and the use of which comes with built-in disaster recovery protection.

We are always alert to the risk associated with the dissemination of our confidential information publicly, especially as it contains highly sensitive details regarding client litigation. In particular, we have focused on the risk associated with attacks on our financial systems. Since our focus is on operating business processes and procedures that minimize the risk of a data confidentiality or cybersecurity breach occurring, we apply significant incremental preventative measures, including, among other things:

- penetration testing conducted by an independent third party;
- quarterly training for 100% of employees;
- routine phishing tests for 100% of employees;
- technical controls over and tracking of document printing;
- restrictions on the use of personal accounts;
- guidelines around the use of social media and restrictions on access to social media and other internet sites;
- registration and enrollment of personal devices with IT tracking of Burford systems access from both company and personal devices;
- prohibitions on local and external drives and non-Burford cloud storage;

- provision of secure password-saving applications for 100% of employees;
- physical security measures across all Burford office locations;
- VPN mandates for staff using public networks; and
- consistent and proactive outreach on cybersecurity issues by senior management.

Incident response and business continuity

As of the date of publication of this Policy, Burford has never had a widespread data breach. We have business-wide Incident Response and Business Continuity Plans, which are structured for each of the locations around the world where Burford has an office as of the date of publication of this Policy and are integrated and interdependent. The Business Continuity Plan also applies to those that perform remote work and those that do not work in any of our established offices. In addition, Burford has an enterprise-wide Incident Response Plan to mitigate the harm caused by a data confidentiality or cybersecurity system breach.

External independent review

Our broader cybersecurity system, Incident Response Plan and Written Information Security Program have been reviewed by an external independent third party.

Training on data security and privacy-related risks and procedures

Preventative measures reflect a view we consistently communicate internally: human error and carelessness are arguably greater risks to data security than sophisticated penetration attacks. Thus, we engage in a variety of training and testing and implement restrictions on technology use to minimize those risks. All Burford employees around the world, as well as contractors and consultants, are assigned web-based cybersecurity training when they join Burford and again approximately every quarter thereafter.

In addition, employee comprehension of cybersecurity within our privacy and data security framework is assessed through quarterly simulated phishing tests and complete annual compliance training that covers the General Data Protection Regulation and other geography-specific rules and regulations. In total, employees spend approximately two hours per year on information technology training, and they must complete cybersecurity training sessions within specified time periods. Violations may result in an employee's account being frozen until the training is completed, and managers are notified of non-compliance.

Responsibility for privacy and data security

In addition, we regularly review best practices from both the legal and financial services industries, including receiving advice from external specialist consultants, and are engaged in a program of continuous improvement. An external independent third party annually reviews our cybersecurity measures, the Incident Response Plan and the Written Information Security Program. We have an internal Cybersecurity Committee composed of senior representatives from across our various geographies and departments. The Cybersecurity Committee has responsibility for privacy and data security and meets regularly to review, benchmark and audit our cybersecurity controls.

A formal internal information technology review is regularly provided to the board of directors by our Chief Information Officer. Importantly, these policies provide escalation points for reporting potential breaches to the Chief Information Officer. If a potential breach were to occur, the Chief Information Officer would escalate to the Chief Executive Officer.

Certification

Our critical platform vendors are certified under System and Organization Controls (SOC), as defined by the American Institute of Certified Public Accountants. Those platform vendors subject to compliance under the Sarbanes-Oxley Act of 2002, as amended, are required to document their protocols and controls to ensure security, including SOC 1 Type 2 reporting on internal control processes and procedures and SOC 2 audit report on technical compliance in specific areas such as data encryption and multifactor authentication. We survey critical platform vendors on appointment and at regular intervals thereafter.

Burford data privacy contacts

For all data protection enquiries, please email info@burfordcapital.com.