dun & bradstreet

Data Privacy, Data Security and Data Ethics Policy Statement

Dun & Bradstreet Holdings, Inc. (the "Company" or "D&B") has adopted this policy statement, which outlines the roles data privacy, data security and data ethics play as core components of the Company's commitment to operate with integrity, both internally and externally. This policy statement applies to all D&B employees ("team members"), and it is approved by senior management and the Audit Committee of our Board of Directors.

In today's fast-paced business world, organizations are seeking more effective ways to leverage data – and associated insights – across the enterprise to improve performance. Data is essential to creating the complete view of customers, prospects, suppliers and partners necessary to power workflows, systems and teams. D&B is cognizant that data collection is complicated, change in data is constant and context is critical. Because data is at the core of our business, we ensure our data privacy, security and data ethics commitments remain top priorities.

D&B maintains comprehensive policies and procedures to protect personal information and other confidential, proprietary and sensitive data against unauthorized access and disclosure that are consistent with our business operations and generally accepted industry standards. These measures include implementing technical, physical and administrative security safeguards, requiring team members to complete privacy and security training and conducting a third party service provider due diligence program to ensure that our vendors employ adequate data security measures while carrying out services on our behalf.

We continually assess our data privacy, data security and data ethics practices and policies. Topics covered in this policy include:

- User Privacy
- Data Privacy & Security Oversight
- Privacy, Security Standards & Audits
- Risk Identification & Response
- Employee & Third Party Expectations
- Data Management
- Data Ethics

D&B's data protection policy is available online in the Data Security section of the D&B Privacy Notice, with summarized information provided below.

User Privacy

Our external privacy notices provide transparency around our collection, processing and sharing of personal information, including information relating to behavioral advertising, user privacy and individual data control rights. All this and more can be found in the following Privacy Notices posted on our websites:

- D&B Privacy Notice
- EU and UK Privacy Notice
- China Privacy Notice

- Canada Privacy Notice
- India Privacy Notice

D&B outlines which users' information is used for secondary purposes in our Records of Processing, which we are building out to cover all data flows across D&B.

Financial Losses Due to Loss of User Privacy

As part of our obligations as a publicly traded company, all material financial losses as a result of loss of user privacy, including losses due to legal proceedings, are available in our public filings with the SEC.

Data Privacy & Security Oversight

D&B has appointed a highly qualified team of privacy professionals including a Chief Privacy Officer and local Data Protection Officers ("DPOs") representing specific geographic regions such as the European Union. Global and regional privacy professionals are tasked with handling any security-related inquiries or incidents. If you have any questions or concerns, we invite you to contact us at PrivacyOfficer@dnb.com or EUDPO@DNB.com.

If you have a security related concern, you can also contact our Global Security and Risk team at security@dnb.com. The Global Security and Risk team members and their associated activities are structured under a framework consisting of the following domains and controls:

- Access Management
- Network Security
- Data Security
- Detection & Response
- System Security
- Software Security
- Validation & Testing
- Awareness & Training

Additionally, our Board of Directors' Audit Committee is responsible for reviewing, with management, policies and practices with respect to risk assessment and risk management. This includes, among others, cybersecurity risks or other data privacy-related risks.

Privacy, Security Standards & Audits

D&B completes several data privacy and security audits annually, including both internal and external third party reviews. We are subject to regular audits by clients, as well as internal audits initiated by compliance team members, sometimes in conjunction with the Internal Audit department. D&B is also subject to regulatory audits and inquiries.

Our information security program framework and control requirements align with various regulations and standards such as DFARS, PCI, ISO, NIST, OWASP and others. Additionally, D&B undergoes the following security audits annually:

- SOC 2 Type 2
- ISO 27001 for UK and Ireland Business Units
- PCI DSS
- EU-US Privacy Shield, Swiss-US Privacy Shield Frameworks
- HIPAA Compliance
- Advanced Technology Partner Status from Amazon Web Services Partner Network
- Regular Customer Audits

- Annual Penetration Tests
- Annual Red Team/Tabletop Exercises

More specific auditing examples can be provided upon request.

Data Breaches and Response

Within the past three years, we have not detected a compromise of D&B core systems leading to unauthorized data access. In 2017, D&B experienced and publicly reported a data breach involving a substantial number of data subjects. Though personal data was involved, the data breach did not expose sensitive personal information and no infiltration of D&B systems was identified. In addition to meeting all our disclosure obligations, significant updates and improvements to our data security safeguards were implemented, including:

- Processes and technology for restricting access to data and systems to authorized individuals
- Barriers and controlled network zones to protect assets from internal and external threats
- Processes and technology to protect the confidentiality, integrity and availability of data at-rest and in-transit
- Monitoring the environment to identify and alert on indications of unauthorized or malicious activity with an effective response capability
- Enforcing secure system configuration and preventative controls
- Enforcing controls to secure applications against misuse and attack
- Evaluating the effectiveness of security controls, processes and their implementation
- Fostering a culture of information security in which users are empowered with the necessary knowledge to protect the company.

Risk Identification & Response

Risk Identification and Prevention

D&B engages a multi-leveled approach to preventing, identifying and addressing data security risks both internally and with the use of third party cybersecurity standards. We safeguard our data by using a combination of preventive and detective technologies such as encryption, virus detection, multifactor authentication, next generation and web application firewalls, automated processes for user access reviews and privilege escalation and intrusion detection systems. Alongside these technical measures, we have policies and procedures in place to communicate and enforce our security controls. Access to data is restricted to authorized personnel by physical and logical access controls.

D&B has developed and maintains practices which establish Information Security Incident classification and prioritization based on the severity of the Incident and the sensitivity of affected systems and data. To support these efforts, D&B implemented and monitors alerts from various tools to provide an effective detection capability. Investigation of alerts and security events, including events related to availability and confidentiality, are conducted to detect new attack patterns as quickly as possible and incidents are declared based on the outcome of the investigation.

Risk Response

D&B investigates incidents relating to security, availability, confidentiality and privacy and responds to any real or suspected breach of security of D&B information systems in a timely, coordinated fashion while complying with applicable laws and regulations. D&B performs security tabletop exercises on an annual basis to ensure organizational preparedness for disruptions.

D&B has implemented the following business continuity strategies to mitigate risks associated with disruption of business operations where possible:

- *Business Continuity Management System:* D&B's Business Continuity Management System (BCMS) enables stability of our operations following a potential disruption or catastrophic event, such as a natural disaster, pandemic, cybersecurity incident, or other events. The plans within the BCMS define objectives, dependencies and processes to limit the impact to those with whom we do business.

- *Crisis Management Team:* D&B has established a Crisis Management Team (CMT) to respond to disruptive incidents by performing a situation assessment, determining the potential impact to the business and coordinating the implementation of response and recovery strategies.

- *Facility Downtime*: D&B enables most team members to work from a nearby D&B facility, or to work remotely from home.

- *Technology Downtime*: D&B maintains an IT disaster recovery program that oversees technology backups and recovery capabilities. Additionally, departments have identified manual workarounds for technology downtime where possible.

- *Third Party Downtime*: D&B has the ability to insource for some third party activities. For other activities, D&B has identified alternate providers or workarounds.

- *Unavailability of Team Members*: D&B cross-trains team members where possible to enable the continuation of work during times when personnel are unavailable. This is supported by documented workflow processes. In addition, D&B attempts to identify personnel in other departments to perform work for increased backup capabilities.

- *Internal Crisis Communications*: D&B uses an emergency notification tool (Send Word Now) that enables mass notification to team members through email, text and phone call.

Monitoring tools are in place to measure current usage against predefined thresholds and generate alerts to notify application and infrastructure support teams when thresholds are exceeded. Alerts are reviewed to determine if corrective action is required. In the event additional information assets are required to address usage needs, they will be deployed in accordance with formal asset deployment and change management policies. Lastly, audit logs

are configured to record significant information, security-relevant activities and events in the D&B systems.

Employee & Third Party Expectations

Employee Policies and Training

All D&B team members participate in annual training on data security and privacy-related risks and procedures as stated in our Code of Conduct. This Code of Conduct outlines best practices for data governance and privacy, including how to collect, store, transfer, classify and use data properly. A more detailed set of policies, procedures and guidelines for team members can be found on the D&B intranet.

D&B team members must complete the required information security training course annually, as well as review, acknowledge and adhere to our Global Information Security Policies. We require comprehensive privacy and security training for all team members as part of our required onboarding process as well as additional training on at least a yearly basis.

Third Party Management

D&B also implements a third party service provider due diligence program to ensure that our vendors employ adequate data collection, processing, transfer, management and security measures in carrying out their services on our behalf. We require the service providers with whom we do business to comply with relevant data privacy, legal and regulatory requirements.

D&B's Partner Code of Conduct lays out expectations for third parties with respect to data privacy, intellectual property, confidential information and more. We expect for all partners to comply with our stated policies and contracts, as well as any applicable local, state, federal and international data privacy laws, regulations, rules and ordinances.

Data Management

Client Data

Maintaining the security and privacy of our clients' confidential data is one of our highest priorities. Once we receive information from clients, we apply our rigorous data privacy and security practices to maintain security on our systems, including any systems accessing or storing client information. D&B has established policies and procedures for securely managing client information, which may be further addressed in our contractual relationship with a customer.

D&B classifies its data as Public, Internal Use Only, Commercial in Confidence, Restricted Confidential and Restricted Sensitive. The permissible use of this data must be understood by the personnel authorized access to the data. We safeguard this data by using a combination of preventative and detective technologies such as encryption and intrusion detection systems. Our policies and approaches with respect to using and sharing personal information varies by product and geography. To learn more, please review How We Maintain Data Security.

Government Data Requests

When necessary or appropriate, we may disclose information in response to a court order, subpoena, law enforcement proceeding, regulatory inquiry or when otherwise legally required to meet national security or law enforcement requirements. In responding to those requests, D&B's response will be limited (a) to the extent necessary to meet national security, public interest or law enforcement requirements or (b) by statute, government regulation or case law that creates conflicting obligations or explicit authorizations.

We have a procedural document (available on the D&B intranet) for Responding to Government and Regulator Requests for Data which sets out our obligations for complying with government data requests while respecting the rights and privacy interests of data subjects.

Currently we do not disclose the number of law enforcement requests for user information, however, we have processes in place to limit the disclosure of personal information to only what is required under applicable law. D&B will provide the minimum amount of information permissible when responding to a data request, based on a reasonable interpretation of the request. Any personal information outside the scope of the request will be redacted.

Data Ethics

Compliance with Laws

On a country-by-country basis, D&B tracks a list of countries where core products or services are subject to government-required monitoring, blocking, content filtering or censoring, while the respective team in each location is tasked with implementing these obligations.

Anticompetitive Behavior Regulation

At the time of drafting this policy, D&B has incurred no monetary losses resulting from legal proceedings associated with anticompetitive behavior regulations. D&B aims to maintain this record by adhering to all anticompetitive behavior regulations and following our robust internal governance policies.