

Privacy, Data and AI Transparency Statement – U.S.



This Privacy, Data and AI Transparency Statement (“Statement”) reflects the privacy, data processing, and data protection standards of the [Responsible D&B Entities](#) in the U.S. This Statement applies to our data processing in the U.S. Information about our data processing in other markets is available [here](#).

- [OUR COMMITMENT TO DATA ETHICS, COMPLIANCE AND PRIVACY](#)
- [OUR VALUES](#)
- [OUR DATA PROCESSING](#)
- [YOUR PERSONAL DATA](#)
- [YOUR DATA SUBJECT RIGHTS](#)
- [COOKIES AND ONLINE ACTIVITY DATA](#)
- [OUR USE OF AI SYSTEMS](#)
- [PERSONAL DATA SHARING AND DISCLOSURES](#)
- [CROSS-BORDER DATA TRANSFERS](#)
- [DATA SECURITY](#)
- [DATA RETENTION](#)
- [RESPONSIBLE D&B ENTITIES](#)
- [HOW TO CONTACT US](#)

At [Dun & Bradstreet \(D&B\)](#), we focus on helping to bring businesses and other organizations together by providing insights about economic opportunities and risks, including data about businesses, business decision-makers and other people who represent organizations of all sizes across industries and sectors around the world. We aggregate data, combine, and generate data, [including scores, ratings, and other analytics](#). Our [Dun & Bradstreet Data Cloud](#) contains data and insights on over 500 million organizations around the globe.

As a responsible data steward for almost 200 years, we strive to balance our commercial obligations and responsibilities with respect for the interests of the organizations and people about whom we process data. As part of this commitment, we aim to be transparent around the ways we process data about people, businesses, and other organizations as well as how we use Artificial Intelligence (AI) systems. Our goal is to improve visibility, engagement, and enrich the overall quality of our data to support meaningful data-driven insights, more opportunities and better business and professional decision-making and outcomes while respecting the interests and rights of individuals and their communities.

How to Contact Us: If you have a question or concern about this Statement, you may contact D&B Global Compliance & Ethics or raise a question or concern using our Helpline. If you are based in other countries, you also may contact us. You also have a right to You also have the right to lodge a complaint or concern with your local data protection supervisory authority. Contact details for data protection authorities are here.

Individual Rights: As described further below, we are committed to respecting the data and digital rights of individuals in both their personal and professional capacities as set forth in our Global Data Subject Rights Policy Statement. You may exercise your rights in connection with our data processing here.

OUR VALUES

At D&B, compliance and ethics begins with human-centered values and principles. The values and principles are set forth in our [Code of Conduct and Ethics](#) and guide us in designing, implementing, improving, disposing, and retiring data processing and management systems in a way that respects human rights, privacy and data protection, non-discrimination, diversity, equity, inclusion, and other applicable legal and regulatory obligations.

Consistent Global Standards

We strive to build and maintain trust through an accountability-based compliance and ethics program that applies to our data processing globally. The following core policies provide the foundation for our program and serve as the basis for our certifications described below:

- [Data Compliance and Ethics](#)
- [Privacy and Personal Data Protection](#)
- [Data Subject Rights](#)
- [AI Ethics](#)
- [Global Cross Border Privacy Management System](#)

Our program has been designed and audited for compliance with ISO 27701, Privacy Information Management Systems (PIMS). In markets in which we are certified as compliant with ISO 27001, Information Security Management Systems (ISMS), we also hold an ISO 27701 certification (PIMS). These certifications are designated on the [global ISO certifications page](#), where applicable.

Since 2016, we have upheld multilateral standards to provide assurance for how we manage our cross-border privacy and data protection obligations and to support our certifications under the following frameworks recognized by regulators:

- EU-U.S. Privacy Shield (2016)
- Swiss-U.S. Privacy Shield (2017)
- EU-U.S. Data Privacy Framework (2023)
- Swiss-U.S. Data Privacy Framework (2023)
- UK Extension to EU-U.S. Data Privacy Framework (2023)
- APEC Cross-Border Privacy Rules System (2023)

OUR DATA PROCESSING

We process many types of data to support business decisioning, including data about

people, businesses, organizations, places, economic activity, sustainability, legal and other significant business events, and third party risks. Some of the data we process is considered [personal data](#). Some of the systems we use to process data are [AI Systems](#).

Dun & Bradstreet, Inc. is registered as a data broker in the U.S. State of [California](#).

Eyeota Pte. Ltd is registered as a data broker in the U.S. State of [California](#).

NetWise Data, LLC is registered as a data broker in the U.S. States of [California](#) and [Vermont](#).

YOUR PERSONAL DATA

What is personal data? Personal data is information that relates to an identified or identifiable individual natural person (“data subject”). Personal data includes information that can be associated with an individual, including data that can be used to identify, locate, track, or contact an individual.

Data that cannot be associated with an identified or identifiable individual, whether it was never associated with an individual (anonymous), or whether all identifiers or links to identifiers have been removed or aggregated in such a way that it is no longer possible to associate the data with an individual (anonymized) is not personal data.

How do we process personal data? The ways in which we process personal data depend on the type(s) of data subject you are, such as your role in engaging with us, your role within your business or other organizations with which you are or have previously been associated, the nature of the products and services that we offer, and our data and analytics methodologies.

YOUR DATA SUBJECT RIGHTS

As detailed in our [Global Data Subject Rights Policy](#), we are committed to respecting the data and digital rights of natural persons in both their personal and professional capacities. In accordance with that Policy and applicable laws, strive to honor the following data subject rights in accordance with well-established public

We provide **Supplemental Personal Data Processing Statements** about our personal data processing activities based on the following data subject groups:

- [Website visitors and online service users](#)
- [Professional contacts in our products and services](#)
- Sole Proprietors in our products and services (*coming soon*)
- [Employees and beneficiaries](#)
- [Job Applicants](#)
- Consumers (*coming soon*)
- [Cookie Policy](#)
- [California Resident Disclosures](#)
- [Eyeota Privacy Center](#)

Each of these Supplemental Personal Data Processing Statements forms a part of the disclosures in this Statement for purposes of the regulatory and framework obligations to which we are subject.

policy principles for individual participation related to data processing and protection, our ethical principles of *Respect* and *Responsibility* set forth in our [Code of Conduct and Ethics](#), rights enshrined in applicable laws, and the value we place on the protection of human rights and civil liberties.

- **Right to Know:** Individual natural persons have the right to know whether D&B processes personal data about them, for what purposes, and other information as required by law.
- **Right of Access:** Individual natural persons have the right to access the specific personal data D&B processes about them and other information as required by law.
- **Right of Correction:** Individual natural persons have the right to correct, update, amend and/or supplement inaccurate personal data that D&B processes about them.
- **Right of Deletion:** Where D&B does not have a legitimate business need to process data about an individual natural person, or where the rights or risk of harm to an individual natural person outweigh D&B’s business need, such individuals have the right to deletion of the data D&B processes about them in accordance with applicable law.
- **Right to Object:** D&B provides direct communications to individuals in accordance with applicable laws. Individual natural persons have the right to object to D&B processing personal data about them and to receiving marketing and certain other commercial communications from D&B.

Additional Supplemental Data Subject Rights

If you would like to exercise your rights with respect to our Eyeota and Netwise businesses, please use the links below:

- [NetWise Consumer Privacy Opt-Out](#)
- [Eyeota Opt-Outs](#)
- [Eyeota Access Request](#)

- **Right to Opt-Out of Commercial Communications:** D&B will honor opt-out requests from individual natural persons related to marketing and other forms of promotional, advertising, or commercial communications.
- **Right to Opt-Out of Data Sale:** Where required by law, D&B will honor specific requests of individual natural persons to opt-out of the sale of personal data about them, including information that identifies them in the products and solutions that D&B licenses to its customers and that is not otherwise publicly available.
- **Right to Opt-Out of Data Sharing with Third Parties for Online Advertising:** If D&B shares data with Third Parties, where permitted by applicable law, for cross-context behavioral advertising or other forms of targeted advertising, D&B will provide and/or utilize readily accessible online mechanisms to enable individuals to opt-out of such data sharing.
- **Right to Withdraw Consent:** If D&B processes data about individuals based on their consent, D&B shall provide transparent and accessible mechanisms for withdrawal of consent that are as easy to use as the method for providing consent.
- **Right to Restrictions:** Individual natural persons have the right to request that

D&B restrict how it processes personal data, including any sensitive data, about them.

You may exercise your data subject rights in connection with our data processing [here](#). Consistent with our [Code of Conduct and Ethics](#), D&B will not retaliate nor discriminate, nor tolerate any retaliation or discrimination, against any individual who exercises rights provided by D&B under our [Global Data Subject Rights Policy](#) or applicable law. Unless a shorter timeframe is required by law or a regulatory or legal obligation applicable to D&B, or an extension is needed and permitted in accordance with applicable laws, D&B will honor requests received pursuant to this Statement and the Policy as soon as practicable and in accordance with the timelines under applicable laws. Except where required by law or a legal or regulatory obligation applicable to D&B, we will not honor multiple or repeated requests from the same individual to exercise the same right more than once every three months.

COOKIES AND ONLINE ACTIVITY DATA

We use cookies and other online data collection technologies, such as single pixel tags, eTags, and scripts, to help you navigate our website and other online services, to remember your selections, to deliver certain features and content supported by third parties and external tools, to measure the effectiveness of our advertising and other marketing activities and to remarket to you after you visit our website. We use two types of browser cookies, session cookies and browser cookies. Some of these cookies and data collection technologies may be placed directly by D&B, and we may permit other cookies and data collection technologies to be placed by third parties. We group browser cookies into three categories: Required, Functional, and Advertising. You can manage your preferences with our Cookie Consent Manager by clicking on “Cookie Preferences” on the footer of our websites at any time. For more information, review our [Cookie Policy](#).

OUR USE OF AI SYSTEMS

We are committed to responsible use of AI, development of AI systems, and implementation of responsible AI solutions that accelerate innovation, improve efficiency, and contribute to sustainable growth. We believe this supports our foundational data compliance and ethics goals of preserving digital trust, reliable data-driven decision-making, and the sustainability of data ecosystems as described further in our [AI Ethics Policy](#).

Our responsible AI program is built on a foundation of our 11 AI Ethics Principles, which guide our approach to responsible AI by design across the AI lifecycle. Our comprehensive approach is supported by shared governance coordinated through our agile AI Governance Council, which brings together expertise from leaders across our business responsible for compliance and ethics, cybersecurity, data governance, data science, intellectual property, and sustainability.

We are committed to transparent, meaningful disclosures about our AI systems in our solutions, processes, and communications. Where we use an AI system to process personal data, we will disclose that in one or more of the following: our Supplemental Personal Data Processing Statements, contextual privacy notices we provide at the point of direct data collection, user guides, model cards, or transparency statements and disclosures related to [scores, ratings, and other analytics](#).

PERSONAL DATA SHARING AND DISCLOSURE

In general, we share data, including personal data, in the following ways:

- With other D&B companies, including subsidiaries, parent companies, and affiliates within the D&B corporate group of companies, including [other markets in which we have operations](#), and in accordance with our [Consistent Global Standards](#).

What is an AI System? We rely on the definition of “AI system” used by the Organisation for Economic Co-operation and Development (OECD)* when referring to “AI” in this Statement to mean a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that [can] influence physical or virtual environments. Different AI Systems vary in their levels of autonomy and adaptiveness after deployment.

**As updated November 2023*

- With members of the [D&B worldwide network](#), which are independent providers of business information around the world with whom we have entered into commercial agreements, including data protection agreements, to support sourcing of data globally as well as distribution of D&B products in the [worldwide network markets](#).
- With our customers, which are businesses and other organizations with whom we enter into agreements to license or access our data via our products and services.
- With authorized resellers whom we permit to resell our products and services.
- With our service providers, including our subcontractors and [subprocessors](#) as necessary to help us carry out our business activities. Service providers that function as data processors, whether supporting our data processing or supporting our data processing on behalf of our customers or others, are only authorized to process necessary personal data as specifically directed by us.
- With other business partners with whom we may enter into strategic relationships to co-develop, co-market, or co-sell certain products, solutions, services, or events. We only permit business partners to process personal information we share as agreed upon by us.
- Through third party cookies and related online technologies that are used by third parties to evaluate use and help us manage the performance of our online services, and for advertising purposes. Please refer to our [Cookie Policy](#) for more information.
- Where required by law or for safety or fraud prevention, such as in the case of a law enforcement seeking information; regulatory agencies investigating a complaint; other form of government investigation, including requests from national security agencies; in response to a court order; in order to investigate, prevent, or take action regarding suspected or actual prohibited activities, including but not limited to fraud and situations involving potential threats to the physical safety of any person; to exercise, establish, or defend our legal rights; to protect your vital interests or those of a third party; or as explicitly required under the provisions of an applicable law or regulation. In responding to such requests, we will limit the information we provide to the extent necessary to meet the requirements of the request.
- In connection with mergers, acquisitions, divestitures, and asset sales where the

[Our Code of Conduct and Ethics for Third Parties](#)

– We expect others who work on our behalf to demonstrate the same commitment that we have made to high ethical standards. Our “third parties” include our suppliers, data providers, vendors, service providers, [subprocessors](#), agents, distributors, business partners, consultants, contractors, licensees, and members of the Dun & Bradstreet Worldwide Network. We consider each third party to be an extension of Dun & Bradstreet and expect them to conduct business honestly and with integrity. We also expect our third parties to choose subcontractors that share our Values and our commitment to conduct business legally, ethically and in accordance with all contractual obligations.

acquiring organization agrees to protections comparable to those set forth in this Statement.

- With other third parties with your consent or authorization in accordance with applicable laws.

Where we disclose personal data about specific data subjects in unique ways, additional information is provided in our [Supplemental Personal Data Processing Statements](#).

CROSS-BORDER DATA TRANSFERS

D&B processes data in the United States as well as in [other markets in which we have operations](#), which we refer to as our Owned Markets. Our transfers are managed in accordance with our [Consistent Standards](#), including the 12 Principles of our [Global Cross-Border Privacy Management System Policy](#) and our intragroup agreements, and are governed by applicable laws, adequacy decisions regarding the protections in countries in which data is received, and multilateral frameworks for transfer and protection of personal data.

Data Privacy Framework

Personal data transfers from the European Economic Area (EEA), United Kingdom (UK), and Switzerland to the United States: D&B legal entities in the United States (the “D&B U.S. Entities”) comply with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. D&B has certified to the U.S. Department of Commerce that the D&B U.S. Entities adhere to the EU-U.S. DPF Principles regarding the processing of personal data received from the EEA in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) under the UK Extension to the EU-U.S. DPF. D&B has certified to the U.S. Department of Commerce that the D&B U.S. Entities adhere to the Swiss-U.S. DPF Principles regarding the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this Statement and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>.

To view the status of our verification, please click [here](#).

D&B U.S. Entities are responsible for the processing of personal data received under the DPF, and subsequently transferred to a third party acting as an agent on behalf of the D&B U.S. Entities. D&B U.S. Entities comply with the DPF Principles for all onward transfers of

personal data from the EU, UK, and Switzerland, including the onward transfer liability provisions.

The U.S. Federal Trade Commission has jurisdiction over D&B's compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF. As described in our Personal Data Sharing and Disclosure Section above, in certain situations, D&B U.S. entities may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

- **For Personal Data other than Employment-Related (Human Resources) Data:** In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, D&B U.S. Entities commit to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF to TRUSTe, an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit <https://feedback-form.truste.com/watchdog/request> for more information or to file a complaint. These dispute resolution services are provided at no cost to you.
- **For Employment-Related (Human Resources) Data:** In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, D&B U.S. Entities commit to cooperate and comply with the advice of the panel established by the EU data protection authorities (DPAs), the UK Information Commissioner's Office (ICO) and the Gibraltar Regulatory Authority (GRA), and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF in the context of the employment relationship.

For complaints regarding DPF compliance not resolved by any of the other DPF mechanisms, you have the possibility, under certain conditions, to invoke binding arbitration. Further information can be found on the official DPF website at <https://www.dataprivacyframework.gov/>.

Cross-Border Privacy Rules System

- **Transfers from APEC Member Economies to other Dun & Bradstreet Owned Markets:** Our privacy practices at Dun & Bradstreet as set forth in this Statement, comply with the APEC Cross Border Privacy Rules System (CBPRs). The APEC CBPR system provides a framework for organizations to ensure protection of personal data transferred among participating [APEC member economies](https://cbprs.org). More information about CBPRs is available at <https://cbprs.org>. If you have an unresolved privacy or data use concern that we have not addressed to your satisfaction, please visit

<https://feedback-form.truste.com/watchdog/request> for more information or to file a complaint. These dispute resolution services are provided at no cost to you.

To view the status of our certification, please click [here](#).

DATA SECURITY

D&B has implemented a comprehensive cyber and data security program to protect D&B data, systems, and assets from loss, misuse, and unauthorized access, disclosure, alteration, or destruction based on the nature of the data and the risks associated with the data processing, taking into account current technology best practices and the cost of implementation.

Our data security functional policies include, but are not limited to the following core policies:

- Acceptable use of Information Assets Policy
- Information Security Management Systems Policy
- Information Security Policy Framework
- Information Security Policy
- Data Handling Standard
- Cryptographic Standard

More information about these functional policies and our cyber and data security program and controls is available in our overview of our [D&B Information Security Control Environment](#).

DATA RETENTION

D&B stores data in accordance with our [Records Management and Data Retention Policy](#), which supports our policies on [Data Compliance and Ethics](#), which sets the baseline standard for data retention at D&B, and [Privacy and Personal Data Protection](#), which requires that Personal data is stored only as long as necessary for the purpose it was collected or otherwise in accordance with any applicable minimum periods defined by law. Where a legally defined period applies, we delete the data in accordance with the expiration of that period.

We define retention periods for D&B data that align with our legal obligations and legitimate business needs. Our data retention periods align with the purposes for which data are processed and the records and systems in which they are maintained. Data retention periods are documented for our data processing activities and systems. Data contained in static records are maintained in accordance with the retention periods for those records. This standard is supported by our [Records Management and Data Retention](#)

[Policy](#), which includes specific retention periods for various types of data and records, including personal data.

D&B LEGAL ENTITIES TO WHICH THIS STATEMENT APPLIES

United States

- Dun & Bradstreet Holdings, Inc.
- The Dun & Bradstreet Corporation
- Dun & Bradstreet, Inc.
- Avention, Inc.
- Dun & Bradstreet Emerging Businesses Corp.
- Dun & Bradstreet Government Solutions, Inc.
- Dun & Bradstreet International, Ltd.
- Dun & Bradstreet NetProspex, Inc.
- Eyeota USA Inc.
- Hoover's, Inc.
- Lattice Engines, Inc.
- MadObjective, Inc.
- NetWise Data, LLC
- Orb Intelligence, Inc.

HOW TO CONTACT US

If you have a question or concern about our privacy, data protection, compliance or ethics practices, you may [contact D&B Global Compliance & Ethics](#) or raise a question or concern using our [Helpline](#).

You also may contact us at us at:

Australia	sydney@eyeota.com
Austria	eudpo@dnb.com
Belgium	eudpo@dnb.com
Bosnia and Herzegovina	eudpo@dnb.com
Canada	complianceofficer@dnb.com
China Mainland	PrivacyOfficerCH@dnb.com
Croatia	eudpo@dnb.com
Czech Republic	eudpo@dnb.com
Denmark	eudpo@dnb.com
Estonia	eudpo@dnb.com
Finland	eudpo@dnb.com
France	contact@getemail.io
Germany	eudpo@dnb.com
Hong Kong SAR	enquiryhk@dnb.com

Hungary	eudpo@dnb.com
India	privacyofficerin@dnb.com
Ireland	eudpo@dnb.com
Italy	eudpo@dnb.com
Japan	complianceofficer@dnb.com
Latvia	eudpo@dnb.com
Liechtenstein	eudpo@dnb.com
Malaysia	complianceofficer@dnb.com
Netherlands	eudpo@dnb.com
Norway	eudpo@dnb.com
Poland	eudpo@dnb.com
Serbia	eudpo@dnb.com
Singapore	singapore@eyeota.com
Slovakia	eudpo@dnb.com
Slovenia	eudpo@dnb.com
Sweden	eudpo@dnb.com
Switzerland	eudpo@dnb.com
Taiwan Region	eservice@dnb.com
United Kingdom	eudpo@dnb.com

Our Legal Representative in the European Union

If you are based in the European Union, European Economic Area (EEA), or your question concerns our data processing activities in the European Union or the EEA, you may contact us at eudpo@dnb.com through the designated representative of The Dun & Bradstreet Corporation, which is D&B Business Information Solutions Unlimited Company based in Ireland.

Dun & Bradstreet Information Solutions Unlimited Company
 The Chase Sandyford Industrial Estate
 Carmanhall Road
 Dublin 18
 Dublin
 Ireland D18 Y3X2

Contacting Your Data Protection Authority

You also have the right to lodge a complaint or concern with your local data protection supervisory authority. Contact details for data protection authorities are [here](#).

Version: 1.1

Effective Date: 25-Sep-2023

Last updated: 17-Dec-2023

Prior Versions:

1.0: https://www.dnb.com/content/dam/web/company/about/content/pdait/DnB_Privacy-Data-AI-Transparency-Statement_USMarket_v1.0.pdf

<https://www.dnb.com/content/dam/web/company/about/content/pdait/DnB-privacy-policy-June-2023.pdf>

Dun & Bradstreet reserves the right to modify, add, or remove portions of the Statement at any time based on changes to its data processing, business, or applicable laws.