PRIVACY & SECURITY OVERVIEW

Data Sourcing

We obtain and generate information through the following means when serving our customers:

Public Sources

Public sources include: public records available from federal, state, local, or foreign governments; open datasets with open data licenses; and information made manifestly public by the consumer or from widely distributed media.

Proprietary Sources

Our proprietary data sources warrant their data is fully compliant with applicable data privacy regulations. Sources come from a variety of verticals, including HR Tech, Real Estate Tech, Identity, Anti-Fraud, Martech and others. PDL actively works with suppliers on compliance-based topics since regulations are changing quickly.

PDL-Generated Attributes

PDL generates various data attributes using metadata, aggregated data, inferences, or predictive models.

Privacy

Ethical data stewardship is at the core of our brand. People Data Labs ("PDL") evaluates all data sources from a compliance standpoint before integrating data from potential sources into our datasets. We evaluate commercial and consumer permissions, and the context of how the data was obtained. We make requests for opt-out, data portability, correction, and deletion where applicable immediate and simple with web forms that are easy to access globally. We also have a strict Acceptable Data Use Policy governing how our data can be used, including prohibited uses.

Sensitive PII

PDL does not sell data categorized as sensitive PII, including certain types of data described in GDPR Article 9 or CPRA 1798.140. For example, PDL refuses biometric, facial, or precise location data.

Global Privacy Regulations

PDL constantly monitors and adjusts to changes in privacy best practices, laws, and regulations. We comply with privacy laws in states, for example, California, Colorado, Virginia, Utah, and Connecticut, in addition to GDPR.

Security

PDL is committed to the safety and security of our customers and their data. PDL performs internal audits at regular intervals to ensure ongoing compliance with NIST 800-53r5 standards. Our infrastructure and software are designed to be compliant from the ground up with GDPR, CCPA, and other privacy regulations. We utilize industry standards from the National Institute of Standards and Technology (NIST) and Center for Internet Security (CIS).

SOC 2
TYPE II
Powered by
Vanta

SOC 2 Type 2

We're proud to announce that we have reinforced our commitment to our customers' security by achieving SOC 2 Type 2 compliance as defined by the American Institute of Certified Public Accountants (AICPA). Read more about SOC 2 Type 2 or download the SOC 3 report.

The information contained in this Privacy and Security Overview is intended as a summary and is qualified entirely by the information contained in our Privacy Policy, Security Policy, and Acceptable Data Use Policy. We encourage you to read those policies, and we welcome any questions you may have on privacy and compliance.

People Data Labs