Perceptyx Privacy Assessment

Perceptyx Privacy Overview

Perceptyx is a cloud-based people analytics and employee experience platform designed to help organizations understand and improve employee engagement, satisfaction, and overall performance. The platform provides a suite of tools for gathering feedback from employees through surveys, polls, and other data collection methods. It uses advanced analytics, machine learning, and artificial intelligence to derive insights from this data, allowing companies to make data-driven decisions aimed at enhancing their workplace culture, increasing retention, and improving employee productivity. Perceptyx acts as a data processor for its customers ("Customer(s)") and provides data protection-related product functionality to allow Customers to best meet their compliance needs.

Customer employees providing personal data will generally provide data in response to a survey initiated by the Customer. The data may include structured or unstructured data, depending on the nature of the survey created by the Customer and will include data categories controlled by the Customer. In most cases, the datasets include some Personally Identifiable Information ("PII") but generally do not include sensitive categories of personal information, unless requested or included by the Customer. When a Customer employee responds to the survey, the Customer's privacy notice applies to the interaction with the employee.

Description of Data Processing

Customers may choose to maintain confidentiality of survey responses with respect to the Customer in the Customer's sole discretion; however, the information the Customer directs Perceptyx to collect is identifiable to Perceptyx in the Perceptyx system. Due to the nature of our product, Perceptyx retains PII related to the administration and response to employee experience surveys, which commonly includes: name, email address, department and title. Perceptyx recommends that Customers not associate survey responses with other sensitive categories of data. Perceptyx does not collect health data, legal data, credit card or other financial account information as part of the survey process, nor does Perceptyx otherwise process such data on behalf of Customers.

Nature and Purposes of Processing

Perceptyx processes data for the purpose of enabling employee listening surveys and associated analysis. Personal Data will be subject to the following basic processing activities: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Subject Categories

Perceptyx generally only collects the information of a Customer's employees. However, Customer may also elect for Perceptyx to collect information from other data subjects, such as contractors or candidates. Perceptyx does not collect data from its Customers' customers, patients, or other similar data subjects.

Categories of Data

Categories of data generally processed by Perceptyx include:

- first name
- last name
- email address
- department
- manager
- location
- Other information that may be requested by a Customer or submitted by an employee as part of a survey

Perceptyx recommends a Customer only request information required for its purpose as required under Article 5, section 1(c) of the GDPR (data minimization).

Special Categories of Data

Perceptyx does not recommend that Customers collect special categories of personal data. These categories of information are generally not required during an employee listening event but may be included if a Customer elects to associate survey responses with these categories. Customers are responsible for obtaining any legally required or otherwise necessary consents to collect and process special categories of personal data.

Transfer Assessment

Where Perceptyx processes personal data governed by European data protection laws as a data processor (on behalf of our Customers), Perceptyx obligations are governed by its Data Processing Addendum ("DPA"). The Perceptyx DPA incorporates the Standard Contractual Clauses ("SCCs") and provides (i) a description of Perceptyx's processing of customer personal data in connection with the provision of the Services, (ii) the types of customer personal data Perceptyx processes and transfers, and (iii) the categories of data subjects (Annex 1); and (iv) description of Perceptyx's technical and organizational measures (Annex 2).

Data Privacy Framework

Perceptyx is enrolled in the Data Privacy Framework ("DPF") as a legal transfer mechanism for transfers of customer data, which may include personal data, outside of the EU to the United States. Customers may view more information about Perceptyx's registration here.

Sub-processors

Perceptyx may transfer Customer data wherever third-party service providers operate for the purpose of providing you the Services. A list of Perceptyx data sub-processors is available in the Trust Center and on our website.

Appropriate Safeguards for Transfers

Perceptyx is headquartered in the US, and has employees in the US, Canada, United Kingdom and several EU countries, which may be used to provide the services. Where Customer PII

originating from the EEA is transferred to Perceptyx, or between Perceptyx group companies or transferred by Perceptyx to third-party sub-processors, Perceptyx will enter into SCCs with those parties.

Laws and Practices

FISA Section 702 ("FISA 702") permits the US government to conduct targeted surveillance of foreign persons located outside the US to acquire "foreign intelligence information." Under FISA 702, the US may compel US electronic communication service providers ("ECSP") to provide such information, which, absent exigent circumstances, must be subject to authorization from the Foreign Intelligence Surveillance Court ("FISC"), an independent judiciary. Perceptyx, like most US-based SaaS companies, could be subject to

FISA 702. In practice, the ordinary customer information processed by Perceptyx is not likely to be of interest to US intelligence agencies. Executive Order ("E.O.") 12333 (unlike FISA 702) does not authorize the US government to compel private entities to disclose or provide access to data. Instead, E.O. 12333 appears to rely on exploiting vulnerabilities in
telecommunications infrastructure in order to collect foreign intelligence, narcotics, or terrorism-related information.

Perceptyx has not received a request for Customer data from governmental authorities. Given the type of data held by Perceptyx, Perceptyx believes it is unlikely such a request would be made.

Security Assessment

Perceptyx maintains SOC 2 Type 2, ISO 27001 and ISO 27701 privacy standard certifications. Perceptyx encrypts data at rest with AES 256. Data in transit is encrypted with tls. Perceptyx follows security guidance, as applicable, from NIST, CISA and NSA. Additional information about our security practices can be found in the Trust Center.

Revision History

Version Date Comment
v. 3 6/30/25 2:15 Ashton Botts and Maria Eubanks: Edited
v. 2 5/9/25 11:39 Michelle Uerling: Formatted
v. 1 12/9/24 3:39 Michelle Uerling: Drafted

Approved: David Hollady