How privacy is protected within PlaetosEQ™

The PlaetosEQ platform is designed to operate optimally without exposing personal identifiable information (PII) or allowing an individual to be associated with any specific content or analysis.

The privacy protections within PlaetosEQ are multi-tiered and incorporate policy, contract and technical layers, which are explained below.

1. **Plaetos Privacy and Information Security Policies**

   Plaetos maintains Privacy policies in conformance with the General Data Protection Regulation and Information Security policies in conformance with the SOC2 information security standard.

2. **Plaetos Customer Contracts**

   Plaetos' customer contracts state explicitly that Plaetos technologies: (i) are not designed to provide insights at the level of individual employees, (ii) contain active protections to ensure employee privacy is protected and (iii) that Plaetos will not attempt to re-identify employees except where required to do so by law.

3. **Treatment of PII in Customer Content** (technical)

   The first step in the Plaetos Machine Learning Pipeline is identification and removal of Personal Identifiable Information (PII) and its replacement with a <PII> flag. The Plaetos PII removal process is built on top of the Microsoft Presidio data protection and anonymization library and is constantly updated to improve its accuracy without compromising data quality through excessive false alerts. PII removed includes: name, email, telephone number, social address, credit card number, SSN and TFN. This PII removal process is under constant review to improve its performance.

4. **Pseudo-anonymization** (technical)

   Employee identities (eg. email, employee number, application user ID) are needed in the ingested data so that demographic and organizational metadata can be correctly linked to employee content. These identities are pseudo-anonymized using a 1-way hash function. This allows future content to be linked to the same employee ID but does not allow reverse-engineering of the ID to identify the employee. Protections from re-identification (see below) operate in addition to pseudo-anonymization to achieve effective anonymization.

5. **Protection from Re-identification** (technical)

   Technical protections within PlaetosEQ are being progressively implemented to prevent employees being re-identified based on demographic or organizational data associated with their content. Protections implemented include: employee ID (original & hashed) cannot be viewed through the user interface (UI); all linked demographic & organizational data is obscured when the number of employee IDs in a document set falls below N (with N set at 10 as a minimum value that can be increased based on data sensitivity and customer requirements).

Updated: 30 November, 2022