PeopleCoral

Data Retention Policy

1. Introduction Our commitment to safeguarding your data is of utmost importance. This Data Retention Policy outlines how we manage, retain, and delete customer data in accordance with industry best practices and principles used by companies on the Microsoft Azure platform.

2. Data Collection and Storage We collect and store customer data necessary to provide our services. This data may include, but is not limited to, organizational information, user profiles, payroll data, performance metrics, and communication records. All data is stored securely in Microsoft Azure's cloud infrastructure, which adheres to strict security standards and compliance requirements.

3. Backup and Recovery We utilize Azure Backup services to regularly back up customer data. Backups are encrypted and stored in geographically redundant locations to ensure high availability and disaster recovery. Backups are performed daily and retained for a period defined by our backup policy.

4. Retention Period The retention period for customer data, including backups, is defined as follows:

- **Active Data:** Data actively used in production is retained for the duration of the customer's subscription to our services.
- **Backup Data:** Backups of active data are retained for a minimum of 30 days and a maximum of 365 days, depending on the selected backup policy.
- **Archived Data:** Data that is no longer actively used but is retained for historical or compliance purposes is archived and stored securely for up to 7 years.
- **Inactive Accounts:** Data associated with inactive or terminated accounts will be retained for a period of 90 days after account termination. During this time, customers can request data export. After 90 days, all data, including backups, will be permanently deleted.

5. Data Protection We implement a variety of security measures to protect your data, including:

- **Encryption:** Data is encrypted both in transit and at rest using industry-standard encryption protocols.
- **Access Controls:** We restrict access to your data to authorized personnel only, using role-based access controls.
- **Regular Audits:** We conduct regular security audits to identify and mitigate potential vulnerabilities.

6. Data Deletion When customer data is deleted in production, it is removed from our active systems immediately. Deleted data may still exist in backups until the retention period expires. Upon expiration, the data is automatically purged from our backup storage. If a customer requests immediate deletion of their data, we will expedite the process in accordance with applicable laws and regulations.

7. Data Access and Requests Customers have the right to access, modify, or delete their data at any time. Requests can be made through our customer support portal. We will process data access and deletion requests promptly, typically within 30 days.

8. User Responsibilities Users must ensure that any data they provide is accurate and lawful. Users are also responsible for maintaining the confidentiality of their account credentials.

9. Compliance and Legal Obligations We adhere to all applicable data protection laws and regulations, including GDPR, HIPAA, and CCPA. Our data retention practices are designed to ensure compliance while providing the highest level of data protection and privacy.

10. Policy Updates This Data Retention Policy may be updated from time to time to reflect changes in our services or legal requirements. Customers will be notified of any significant changes to this policy.

11. Data Breach Notification In the event of a data breach, we will notify affected users promptly and take appropriate measures to mitigate the impact.

12. Termination We reserve the right to terminate or suspend access to our services for violations of these T&Cs.

13. Contact Information For any questions or concerns regarding this Data Retention Policy, please contact our Data Protection Officer at info@peoplecoral.com.

Data Privacy Policy

1. Introduction We are committed to protecting the privacy and security of our customers' data. This Data Privacy Policy explains how we collect, use, store, share, and protect your personal and organizational data when you use our software and services.

2. Data Collection We collect data that is necessary for providing our services effectively. This may include:

- **Personal Information:** Such as names, email addresses, phone numbers, and job titles.
- **Organizational Data:** Such as company name, organizational structure, payroll information, performance metrics, and other HR-related data.
- **Usage Data:** Information on how you use our services, including IP addresses, browser types, access times, and pages viewed.

3. Use of Data The data we collect is used to:

- Provide and maintain our services.
- Improve and customize our software to better meet your needs.
- Communicate with you regarding updates, support, and other service-related information.
- Ensure compliance with legal and regulatory requirements.

We do not sell or rent your personal data to third parties.

4. Data Sharing We may share your data with:

- **Service Providers:** Trusted third parties that help us operate our services, such as cloud hosting providers, payment processors, and customer support tools. These providers are bound by strict confidentiality agreements.
- **Legal Authorities:** If required by law, we may disclose data to comply with legal obligations, respond to lawful requests, or protect the rights and safety of our customers and others.

5. Data Protection We implement a variety of security measures to protect your data, including:

- **Encryption:** Data is encrypted both in transit and at rest using industry-standard encryption protocols.
- **Access Controls:** We restrict access to your data to authorized personnel only, using role-based access controls.
- **Regular Audits:** We conduct regular security audits to identify and mitigate potential vulnerabilities.

6. Data Storage and Retention Your data is stored securely on Microsoft Azure's cloud infrastructure. Our Data Retention Policy outlines how long we retain your data and the procedures for deletion after the retention period expires or upon your request.

7. Your Rights You have the following rights regarding your data:

- **Access:** You can request a copy of the data we hold about you.
- **Correction:** You can request corrections to any inaccurate or incomplete data.
- **Deletion:** You can request the deletion of your data under certain conditions.
- **Portability:** You can request a copy of your data in a structured, machine-readable format.

To exercise any of these rights, please contact our Data Protection Officer.

8. Cookies and Tracking We might use cookies and similar tracking technologies to enhance your experience, analyze usage, and personalize content. You can manage your cookie preferences through your browser settings.

9. Compliance with Laws We comply with all applicable data protection laws, including GDPR, CCPA, and other relevant regulations. Our data practices are designed to meet the highest standards of privacy and security.

10. Changes to This Policy We may update this Data Privacy Policy from time to time to reflect changes in our services or legal requirements. We will notify you of any significant changes through our website or via email.

11. Contact Information For any questions or concerns regarding this Data Privacy Policy, please contact our Data Protection Officer at info@peoplecoral.com.