DATA SECURITY & PRIVACY POLICY

PROCLOZ

CONTENTS

1. Policy brief & purpose

Maintaining the security and integrity of customer data is a high priority and we endeavour to maintain appropriate administrative, technical, personnel and physical measures to safeguard personal data against loss, theft, and unauthorised uses or modifications. Procloz's Data Protection Policy refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality. With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

2. Scope

This Policy applies to all Procloz employees, contractors, vendors, interns, associates, customers and business partners who receive personal information from Procloz, who have access to personal information collected or processed by Procloz, or who provide information to Procloz, regardless of geographic location. All employees of Procloz are expected to support the privacy policy and principles when they collect and/or handle personal information, or are involved in the process of maintaining or disposing of personal information.

3. Data Protection Policy Coverage

Employees of Procloz must follow this policy. Contractors, vendors, interns, associates, customers and business partners are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data. We expect you to contribute to the security culture of our company by following appropriate security policies and procedures, completing assigned trainings, and reporting suspected incidents to relevant incident response contacts promptly.

4. Policy elements

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc. We keep records of your personal data no longer than necessary for the purpose for which we obtained them and for any other permitted compatible purposes, including compliance with legal obligations in the field of employment law.

Procloz collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties

Data will not be:

- Communicated informally
- Stored for more than a specified amount of time
- Transferred to organizations, states or countries that do not have adequate data protection policies

- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data Procloz has direct obligations towards people to whom the data belongs. Specifically we must:

- Let people know which of their data is collected
- Inform people about how we'll process their data
- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases

5. Actions

To exercise data protection Procloz is committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in data privacy and security measures
- Use SFTP (Secure File Transfer Protocol) to exchange data
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (secure data transfer, NDAs with contractors and business partners, limited employee access, data encryption, secure emails, document shredding, secure locks, frequent backups, access authorization etc.)

6. Third Party Software Security Policy

We will also seek to ensure that any third-party service providers we use to administer our Human Resources programmes, are bound to maintain confidentiality when handling your personal data on our behalf, in a manner that is consistent with this Policy. Please find below Data Privacy Policy link for review –

https://www.greythr.com/privacy-policy/

7. Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action. Any individual who accesses, uses or manages Procloz's information is responsible for reporting data breach and information security incidents immediately to the contact below.

8. Contact

To exercise your data subject rights, or if you have questions about this Policy or report a data breach incident, please send an email to: contact@procloz.com