SOCIUS

– business tools for nonprofits –

SOCIUS DATA PROTECTION POLICY

[Last Updated: 26 July 2019]

Data protection is an essential legal compliance matter for Socius Holdings (Pty) Ltd. *(referred to herein as "Socius", "we", "us", or "our")* and we are committed to complying with the current international and European data protection laws including GDPR & PECR. This Data Protection Policy *(referred to herein as "Policy")* describes how Socius, as a data controller, collects, processes, transfers, stores, and protects personal data pertaining to its clients and their stakeholders. This Policy applies to all clients of and recipients of information provided by Socius.

We will only deal with your personal data in accordance with the terms of this Policy, which are reviewed frequently. Please revisit the documents available on our website for up to date policies. For more information on privacy and non-client-specific data handling, please consult the Socius Privacy Policy.

Core Principles

Socius is committed to processing data in accordance with its responsibilities under data regulations. Article 5 of the GDPR outlines the following core principles, declaring that data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Sub-Processors

Very few modern companies are fully self-sufficient and so use of trusted third parties is essential to maintaining our business. We maintain a list of any and all sub-processors who assist Socius in the provision of the services. In order to obtain a list of our trusted sub-processors, please contact us at contact@socius.ch.

In the provision of Socius services we will naturally need to act as a sub-processor of your data and that of your constituencies. Where this is the case, Socius handles all data in accordance with this policy. Where clients have data processing requirements that might be considered out of the ordinary and are not covered by this Policy, the client is responsible for informing Socius of such in order that we may take special care to remain compliant with your policies.

Client Responsibilities

In dealing with Socius, it is your responsibility to ensure that:

- positive consent and/or legitimate interest/professional relevance is clearly documented in your records before Socius receives the data;
- data protection policies and practises are maintained that are GDPR & PECR compliant; and
- all data should be sent to Socius in compliance with your secure transfer standards.

Security

Socius will store and process your data in a manner consistent with industry security standards. We have implemented appropriate technical, organisational, and administrative systems, policies, and procedures designed to help ensure the security, integrity, and confidentiality of your data and to mitigate the risk of unauthorised access to or use of your data.

Processing: Socius staff are contracted to keep your data confidential whilst being processed. All data processing takes place in password-protected files. We will only process personal data based on the documented project objectives, and not for any other purposes.

Storage: During the course of Socius handling client data, contact and personnel data is stored securely in password-protected files, both offline and on Cloud-Based Storage Systems (Google Drive & Onedrive). Socius also has clear procedures for the use of Cloud-Based Storage Systems is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. Socius will ensure that it is satisfied with controls put in place by remote / cloud-based data services providers to protect the data. Socius will return your data at the end of the project or working relationship and delete all records from our systems, once you have confirmed receipt of the data and confirmed that we can delete it.

Transfer: Socius will only transfer data internally and to clients as encrypted files. When Socius sends a client encrypted data files by email or by sharing access to cloud-based documents, the passwords for decryption will be shared separately and confidentially, by way of email to the client's named liaison (the contract signee, unless otherwise agreed) only.

In the unlikely event that Socius becomes aware of any unauthorised or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of personal data related to your project *("Security Incident")*, Socius will take reasonable steps to notify you without undue delay, but in any event within 72 hours of becoming aware of the security incident. Socius will also reasonably cooperate with you with respect to any investigations relating to a Security Incident with preparing any required notices, and provide any other information reasonably requested by you in relation to any Security Incident.