Small Improvements Privacy and Security: Guidelines and Policies

This document is an overview of our internal guidelines and policies.

Data Privacy Guidelines **1**
- Preamble 2
- Data scarcity 2
- Data transfers and subprocessing 2
- Data anonymization 3
- Least access principle 3
- Legal 4
- Review and Update 4

Access Control and Authorization Policy **5**
Data/Security/Privacy Incident Response Plan **6**
- Incident Severity 6
- Step 1: Ring the alarm 6
- Step 2: Fix & preserve 7
- Step 3: Document & inform 7
- Step 4: Post-mortem 7

Data Storage and Retention Policy **8**
- Data Storage 8
- Data Retention 8

Replication and Data Backup Policy **10**
- Backups 10
- Requirements 10
- Implementation 10
- Replication 10

Anti-malware and virus policy **11**
- Overview 11
- Pre Approved installable tools 11

Physical and Environmental Security **13**
Laptop, Mobile Device and Removable Media Security Policy **14**
- Guidelines 14

Password Policy **15**
Email Security Guidelines **16**

Data Privacy Guidelines

Preamble

Almost all of the data we process on behalf of our clients is highly sensitive. Our entire business depends on us keeping our customers' data safe. If we ever lost a single customer's data, the news would spread and instantly erode trust in our company. No amount of savings could help the company recover. Data privacy is our topmost priority.

On the one hand we need to spend considerable effort on technical means to ensure data security, so no adversary can find loopholes and extract data. But it also extends to the way we handle the data ourselves. Our internal processes need to be strict to the point that they feel "too strict", so that accidental data loss becomes impossible too.

As a result, every single team is responsible for data protection, not just our Data Protection Officer.

Data scarcity

We make sure to only collect the least possible amount of data needed to achieve essential business goals. The data our customers enter into SI is already highly confidential, but that doesn't mean we should collect even more data just for the sake of it. We never collect data on the grounds that it *might* be useful in the future.

Data transfers and subprocessing

Our core data lives in the highly secure Google Cloud. To provide high quality service to our clients, we need to make use of additional tools though: Finance, Customer Support, Sales, Marketing and Development all need to use dedicated tools to work efficiently, and for this we need to share some data with those tools.

It's morally the right thing to do to share as little data as possible with subprocessors, and it also makes business sense. If one of our sub processors got attacked, we don't want this to risk our own company. So we strive to share as little data as possible, typically only admin names and email addresses. In cases when more transactional data has to be shared, like when SI needs to send an email about someone's performance review, the mail should still contain as little content as possible ("your manager has shared your performance assessment, click here to read it" rather than "your manage has shared your assessment and we enclosed it within this email").

We only work with highly respected vendors that have been in the business for years and have a good track record regarding outages, breaches and overall behavior. The list of subprocessors can be found on our website: https://www.small-improvements.com/subprocessors/

Before starting to track new data (especially PII) or especially before sharing any additional data with (potentially additional) subprocessors, we ask ourselves if this is strictly necessary to solve our customers' needs and to achieve our business goals. If not, then we'll avoid the project entirely. We inform customers about changes to subprocessors upfront, we sign DPAs with subprocessors, and we strive to give customers as many options to opt out from subprocessors as possible.

In summary, we select as few sub processors as possible to get the job done, and we share only as much data with them as is strictly necessary, and we ensure we have GDPR-compliant DPAs in place before sharing any data with them.

Data anonymization

Wherever possible, we'll anonymize data. However, since we typically only share the minimum of data with subprocessors, and since we typically only run very dedicated reports in order to solve specific challenges, data anonymization doesn't (need to) happen as often.

As an example, we use an external service to improve search performance for a specific type of search, and we only share User IDs (but not user names, email addresses or the like) with that service to perform those specific searches. So we don't even need to perform anonymization for this usecase.

But in cases where data anonymization is possible and feasible, and can't easily be replaced by a data scarcity/minimization approach, we'll anonymize or pseudonymize data.

Least access principle

We ensure that every employee only has access to data they strictly need to know in order to get their job done. This makes it considerably harder for an intruder: If a hacker managed to compromise the account of (say) our accountant, they'd still not have access to the database or codebase, since the accountant doesn't have access to the database. This applies also the other way around.

The principle also makes it a lot less likely that someone accidentally shares sensitive information, for instance in an email attachment that goes to the wrong recipient. The details are explained in our Access Control and Authorization Policy.

We have internal role-based permissions to restrict access to only those who need to be able to access a set of information. We review role- and group- membership of staff on an ongoing basis, and also each time we hire or off-board a person. team.

Legal

We employ a Privacy Policy/Obligation to Data Secrecy according to German Law that all employees need to sign, which binds them to maintain the confidentiality of all personal and private data. Violations can result in fines and imprisonment.

Review and Update

It's our policy to always maintain compliance with applicable legal, regulatory, and contractual obligations related to information security requirements. Our DPO continuously provides us with new insights and updates relating to legal changes and relevant court decisions, and we'll ensure to implement required changes in our business model swiftly.

Access Control and Authorization Policy

We manage highly confidential customer data, our own financial data, and plenty of our business plans and goals. The moment adversaries get access to this data, our entire business is at stake. We need to ensure that we only use systems we trust, and that we only give access to staff we trust.

In addition though, it's important to remember that even a person we trust may have their account breached by intruders. So even the most trustworthy staff member should only get access to just as much data and applications that they can do their job well, and also only for the time they need and but not longer ("least privilege principle")

Some practical guidelines:

- Never share any crucial passwords between staff. Only use and commission new systems that support multiple user accounts
- Make sure you enable 2-factor authentication when dealing with important data, especially if you're an admin, but also when possible as a normal user. Example: Even as a contributor (e.g. non-admin) for the website, your account could be misused to link to malware sites.
- The main admin accounts are assigned by the CTO by the Information Security team. For each system we also have system-owners who are in charge of assigning new users when needed.
- If API keys have to be used to access another application from within SI, treat those API keys like a password and don't share it widely, only store it inside 1Password and only share with the people who really need to know
- As an admin to any system, make sure that you only assign additional access (both in terms of new users, and in terms of added privileges) only on a strict need-to-know basis. Check with the system owner, or with the Information Security Team (or with the CTO) if in doubt.
- Always consider handing out permissions temporarily. Someone might only need access for a week. Revoke the permission after a week then.
- The Information Security Team routinely revisits all systems and removes people who don't require access anymore. If in doubt, we'll err on the safe side. So if your account was downsized or removed by accident, please let them know, it was not done with bad intentions, we'll reinstall your permissions so you can do your job

Data/Security/Privacy Incident Response Plan

Incident Severity

When in doubt start with high severity and do post in #incidents immediately. We can always downgrade and call All Clear.

High

We have indications or reports that data or security or privacy has been breached or that an exploit or defect is putting us at risk – e.g. hackers can access data, companies or users are seeing data they shouldn't etc. Stays High if we have confirmed that this is indeed possible.

Priority: Drop everything and react immediately.

Medium

We have identified that the issue is not exploitable or not actually within our system, or that there is a user error/UX issue at play.

Priority: Can be addressed the next day, and either moved into follow-up ticket (bugs or tech roadmap) if risk assessment warrants this, or closed (if false alert).

Step 1: Ring the alarm

- Immediately inform everyone in the #incidents Slack channel. Specifically inform the Information Security team and the CTO too.
- Have a call as soon as possible
    - Describe:
        - severity
        - who reported the incident when via which channel
        - scope (type and amount of data potentially at risk, global or for a single customer…)
        - any details known
    - Determine incident owner, and who is part of the team responding
    - Clarify expectation for response time

If there is indication for a data breach or major security incident, also inform our Data Protection Officer – she can help figure out if the incident needs to be reported to authorities or not.

If in doubt, it's better to get a few people too many involved than missing out on that one person who could have had the great idea. Efficiency doesn't matter, speed and effectiveness matter most.

Step 2: Fix & preserve

- Take systems affected offline if a data or security breach that can be exploited further is suspected
- If a customer account is specifically affected and might be leaking data, lock it
- Preserve any evidence forensics about the breach if external influence
    - Google request logs with a time stamp and IP address
    - Internal log messages
    - our audit records
- Analyse whether this issue could affect and endanger neighboring systems
- Investigate root cause and fix

Step 3: Document & inform

- Document the incident thoroughly
- if data has been leaked or security has been breached,
    - Customer-Team: notify affected or at risk customers within 8h with details on the scope of (potential) breach, an update on the situation, and a timeline when to expect the next update
        - using email, intercom, and consider in-app messages
    - inform our Data Protection Officer (do not skip this step!!!)
    - document EVERYTHING as you do it
- if applicable (e.g there is a security breach on premises) notify law enforcement agencies

Step 4: Post-mortem

- Run a thorough post-mortem with actions to prevent this type of incident in the future. An example of a previous incident's post-mortem can be found here.

Disaster Recovery Plan

As outlined in our Business Continuity Plan, there are plenty of threats to Small Improvements: Banks can collapse and leave us without access to our savings, the office could burn down, our third party service providers could get wiped off the internet, staff could find themselves without access to electricity or internet, or select key people could resign or even die. While each of these threats would be tragic if they incurred, neither have the potential to truly harm the company itself, Small Improvements would work around it and recover.

The only truly large risk we see is that our core database in the Google Cloud is harmed, either by a general attack on Google, or by a hacker getting into our system and wiping the data from within.

In order to mitigate this risk, we store backups on separate servers. These backups are also in the Google Cloud, but on an entirely different system, so that the chance of both being wiped out at the same time has to be considered negligible. If the worst case happens and the database is harmed or wipe, we can easily restore a backup. See our backup & replication policy for additional detail:

Restoring a backup into existing infrastructure is easy, but during a true disaster it's conceivable that our entire Cloud Service has been wiped. In that case, a single developer can still install a new service based on instructions and configuration that's stored in our code repository. The process is documented here (internal link). It would require some additional adjustment from our DNS system, but even this extreme case of building a new Small Improvements service from scratch won't take more than one business day.

Data Storage and Retention Policy

Data Storage

Our customer data is highly sensitive and we spend a lot of effort to keep it safe from data loss, breach and disruption. The efforts range from careful hiring over defensive coding, automated testing, intense code reviews to a continuous penetration testing program and to careful handling of the data by staff. The following outline some of our practices and commitments.

Data encryption

All data is encrypted during transit using HTTPS/SSL. All data is encrypted by default in the Google Data centers, by Google. In addition, we encrypt string-based content such as the

written feedback, objectives, performance reviews in the database on a per-field basis, using symmetric AES-256 encryption, making it even harder to analyze the data in case of a database breach.The encryption/decryption process happens on the server, at the so-called service level, before and after accessing the database. A different key is user for each client, making the logical separation of data even more pronounced.

Customer data is stored logically separated from each other in the databases, and only pseudonymized or anonymized data will be used for test purposes. Development and QA environments are entirely separated from the production database.

Data avoidance

We collect only the data that we need to be able to provide the service, and we're especially careful regarding data sharing with other providers.

We work hard at keeping the list of our subprocessors as small as possible, and we only share the absolute necessary amount of data with those processors. The core employee data is stored in the Google Cloud, and we only share as much PII employee data that's required to be able to send email notifications with our email provider. Other than that, the other sub processors only process data about users that interact with us – for instance during the sales process or when solving a support ticket. All of the highly confidential data does not leave the main database in the Google data center.

Data access

We employ internal role-based and user-based permissions to restrict access to only those staff who need to be able to access a set of information (need-to-know basis). We revisit access levels regularly and choose the minimum levels possible.

Access to functionality like large-scale exports from our product is only available to special role members, and must be made available manually by our Customer Success team.

Data Retention

It's our policy that customers decide when they want to either delete individual pieces of information, or when they want to close their account and delete all data. We don't interfere with customer data at all, and don't delete anything except if asked by customers.

We advise customers to remove any data that they don't need anymore on a regular basis. This applies especially to former employees and old reviews. It's easy to download PDF versions of old reviews and store them on site if needed, so that former employees can ultimately get deleted from Small Improvements if this is desired by the customer.

Please note that even after data is deleted from the active database, the data remains accessible in backups for up to 6 months. See our Replication and Data Backup policy for more information.

Deletion of a customer account by the customer does not automatically erase the data from our subprocessors. Email metadata will live on for 30 to 60 days at our email sending provider, and if you'd like to erase the remaining data also from our CRM and Support system, please notify us at support@small-improvements.com.

The only exception to data deletion is that our German entity has a legal requirement to store invoices and credit notes for at least 10 years, so that information can't get erased even when a customer requests it.

Replication and Data Backup Policy

Backups

It's crucial we keep backups of our core production data, so in the event of major failure (like a coding error that erases customer data from the database) we can roll back to a previous safe state.

Requirements

- We take daily snapshots of all production data and store it on an independent system.
- We get notified in case a backup didn't succeed
- We replay backups frequently in order to ensure they are still working
- We delete backups after 6 months

Implementation

- Our Application runs in Google Cloud App Engine, the live database being in Google Data Store. Our backups are stored in the Google Cloud Storage service, which is entirely independent. Even if a coding error or App Engine related problem led to our entire database being wiped, we'd be able to recreate the database within hours.
- A daily notification mail sent to key employees when a backup has been taken, and in case anything in the process has failed the email states this very clearly in the subject line, and we'll take immediate action to ensure the backup will work
- At least every 2 months we take a backup and replay it onto an empty server and ensure the process still works
- Backups are deleted after 6 months

Replication

Goal

- It's important that we don't have a single point of failure. All our production systems need to survive individual servers or even entire data centers going down

Implementation

- We run all of our crucial production systems in the Google Cloud. Most services have cross-datacenter replication built in by default (our database and production servers for instance). In the few cases where we have to build our own infrastructure like our Google-hosted Load Balancers, or our Google-hosted PDF-generation-servers, we ensure that there is always enough replication in place for single servers or even datacenters to fail without jeopardizing the service itself.

Anti-malware and virus policy

Overview

It's crucial our computers are not getting infected with malware, since that would bypass *any* of our other security measures. To achieve this, several measures are required

- The biggest threat to an already security-conscious organization like Small Improvements is malware that disguises itself as useful software. Any small useful utility (like a timezone conversion tool, or audio-player) can turn out to be spying on the user, or – even if not harmful today – get hacked eventually and turn into Malware. Therefore employees are requested to install software from trusted vendors only, from vendors that have been pre-approved by the company, or approved on the spot by their team's Team Lead. The goal is to minimize potential attack vectors, so don't install software on work computers unless it's required to do the job, and unless you know a software has approval from the company. You may always request access to new software of course, but the company needs to know and approve.
- Another key attack vector is malware sent by mail: Everyone is required to be very skeptical at any unsolicited mail, and at any odd-sounding mail that requires to open attachments of click links. Even coworkers' mails need to be viewed with scrutiny to avoid falling victim to a coworker who has been hacked and starts sending malware mails
- Further Malware attack vectors are dodgy or breached websites. Only go online with up-to-date browsers that are considered safe, like Chrome, Safari, Firefox, or Edge, and avoid sites that are neither work-related nor informational
- Firewalls: Every employee is required to enable their operating system's firewall and keep it enabled
- Antivirus: Any computer with an operating system prone to viruses (essentially meaning all Windows computers) need to run up-to-date Antivirus software. The company will make recommendations as to what software to use. Apple and Linux computers are exempt from this policy since viruses are effectively prevented by the operating system, and no antivirus software provides better support than the built-in mechanisms.
- Operating system updates: Every employee is required to keep updating the operating system at all times. This is usually easy since the OS prompts the user, but one still has to accept the update, and everyone is required to do so whenever feasible.

Pre Approved installable tools

This is a non-exhaustive list of pre-approved software. We update this list frequently internally, but don't necessarily update it on the website immediately. We merely provide it as an indication of how we work.

- Adobe Products
- Apple Products

- Microsoft Products
- Google Products
- Design tools: Sketch, Figma, Skitch
- Dev Tools: Jetbrains & Github products, JProfiler, Emacs, vim, and comparable popular and trusted dev tools
- Mail: Thunderbird, Evolution
- Browsers: Chrome, Firefox, Opera
- Productivity: Slack, Zoom, Goto-Meeting
- Music: VLC Player, Spotify, Soundcloud

Physical and Environmental Security

Unlike more traditional companies we don’t have any secrets in our office. We don’t have local servers, we don’t print out customer data, and all our computers are encrypted. Also, we’re a very tight-knit team, we rarely have visitors, and our office is very separate from everyone else in the building. We don't need a reception desk, visitor badges, or electronic sign-in procedures.

Still, security is crucial, and it's conceivable that an intruder could somehow use information gleaned from the office for social engineering purposes ("How does the printer work again? (...) Ah, now it works. Also, can you help me with the password for SI?"). Therefore we still need to be strict and careful. So our physical guidelines are as follows:

- Our office has very solid doors, these doors have to be closed at all times, so that visitors need to ring the bell in order to enter.
- When you greet visitors, always ask them who they would like to meet, and then walk them to that person personally.
- As the host, ensure you guide your visitors all the way to the doors, and ensure you close the door after them personally.
- When you have visitors, inform the entire office by sharing it in our #berlin-office channel
- It’s fine to occasionally bring friends to the office, but ensure you properly introduce them, and don’t let them hang around on their own.
- If you see unattended strangers in the office, ask them (in a friendly way) who they are here to meet with. Check back with that person, and ensure that the next time we improve the process so that strangers are always attended (or properly introduced).
- Everyone has to take their laptop computer home with them. While all data is encrypted, we'd still need to be extra safe and temporarily lock down accounts and rotate passwords, and if this happened to several people at once, potentially parallel to a cyber attack or general incident that requires all hands on deck, then we'd be in trouble.
- The last person leaving the office is responsible for double checking the windows, rolling down the roller shutters, and ensuring both doors are properly locked.

Laptop, Mobile Device and Removable Media Security Policy

Small Improvements employees are provided with a laptop to perform their work duties. Most of our security practices are outlined in other documents and policies, this document is mainly an excerpt of the rules that apply to mobile and removable media devices specifically. Please refer to the security code of conduct, password policy, and general security policies for the broader picture.

Guidelines

- All devices and removable media have to be protected by a strong password that is not being used elsewhere by the employee.
- All devices and removable media have to be encrypted.
- Firewalls have to be enabled, antivirus and antimalware products have to be enabled when available, and the operating system and browsers have to be updated continuously by the employee.
- Devices need to get locked manually once the employee leaves them unguarded. Devices have to be configured so they automatically lock down and require re-entry of the password after at most 5 minutes of inactivity.
- Sensitive data may only be stored on local or removable devices for a long as necessary to perform the desired work result, and has to get deleted thereafter.
- Loss of any device needs to be immediately reported to management of Small Improvements.
- Any work-related documents created or edited on these devices remain the sole property of Small Improvements.
- Any device that will be reused or disposed (laptop, USB stick etc) needs to be *securely* formatted before doing so.
- Company-owned laptop computers and mobile devices *may* be used for private usage within limitations. Our security code of conduct provides more detailed information.

Password Policy

Security is paramount at SI, and using the right passwords is one core ingredient. Please follow the following guides and requirements carefully:

- It's crucial that every employee uses **one-time passwords for every business service** they use on behalf of SI. Never use a password directly that you can remember, or (worse) that you've been using on another system. Instead, use a password manager such as 1Password (or the Apple Keychain) that will generate passwords, and store them for you. Choose a **strong master password** for 1Password and remember that one (and make sure you never use it anywhere else either)
- When setting passwords, **choose at least 14 random characters**, and unless the service prohibits this do include digits and special characters too
- Since we use one time passwords, we don't have to cycle passwords. If one service we use was compromised, change that password, but there's no need to change anything else.
- **Multi-Factor** authentication should be used whenever possible. It *must* be used on all systems that enable access to confidential data (like customer data), and it must also be used systems where your access level could be exploited to cause harm (if you have edit rights to the website for instance : the website has no customer data, but installing malware on the website would of course be disastrous still)
- **Do not share personal passwords!** The only possible exception is if we use a service that simply doesn't allow multi-user access, like Instagram for instance. In that case, create a secure "vault" in 1Password and share the password only with the people who absolutely need access. Change the password once a person doesn't require access anymore (or is leaving the company)
- **Change initial passwords immediately:** In some cases we will set up a new account on behalf of staff and we *have* to assign an initial password. Most systems require the new employee to change the password immediately. In case the system does not mandate this, it's on the employee to set a new secure password.
- **If in doubt, change your password!** If a service you use has been compromised, or *may* have been compromised, immediately change your password.

If you have questions about this policy, don't hesitate to ask your manager, or even the CEO.

Email Security Guidelines

Email is by default not a secure communications mechanism. Emails are transmitted in plaintext, and there is no guarantee that the person pretending to send a mail is actually that person, nor that your mail will reach the right person. A lot of our communication has moved from Mail to internal tools like Slack, Trello or Confluence – but even so, mail remains a common part of our work lives, and there are risks associated with every attachment we view, every link we click, and any information we read (and which may or may not be true..)

Guidelines

- Trust nobody. When reading or sending mail, always consider the worst. What if it's not a coworker sending an interesting file, but actually an adversary who wants you to install some malware, or get confidential information out you via social engineering? If in doubt, always double check in person, via phone, or at least via Slack.
- Don't share confidential information via unencrypted mail. It's very easy for adversaries to read unencrypted mail. Either set up encryption, or merely use mail as a notifying mechanism for data that you have sent some other way ("I've just sent you the information via Dropbox/Fax/Slack").
- Do not encrypt a file and then send a second mail that contains the password. This is almost as silly as not encrypting the file at all.
- When possible, avoid using mail, but resort to using internal tools like Slack for direct or group communication, and Confluence for bigger topics and company-wide discussions. The risk of someone *pretending* to be your manager or your coworker on Slack is much smaller than in mail, and the risk of someone spying is smaller. (Naturally, even notes and information shared via these systems have to be treated carefully. A coworkers's Slack account may have been compromised, so remain cautious if someone suddenly shares a file like "all employee salaries" with you. There's a good chance that even this is malware.)
- When possible, even invite external partners into a shared Slack channel, rather than sending information via mail.
- Sometimes customers want to send us data. Encourage them to use more secure systems than sending mail. Customers shouldn't send their employee data via unencrypted mail to us either, they should be using secure tools themselves too.