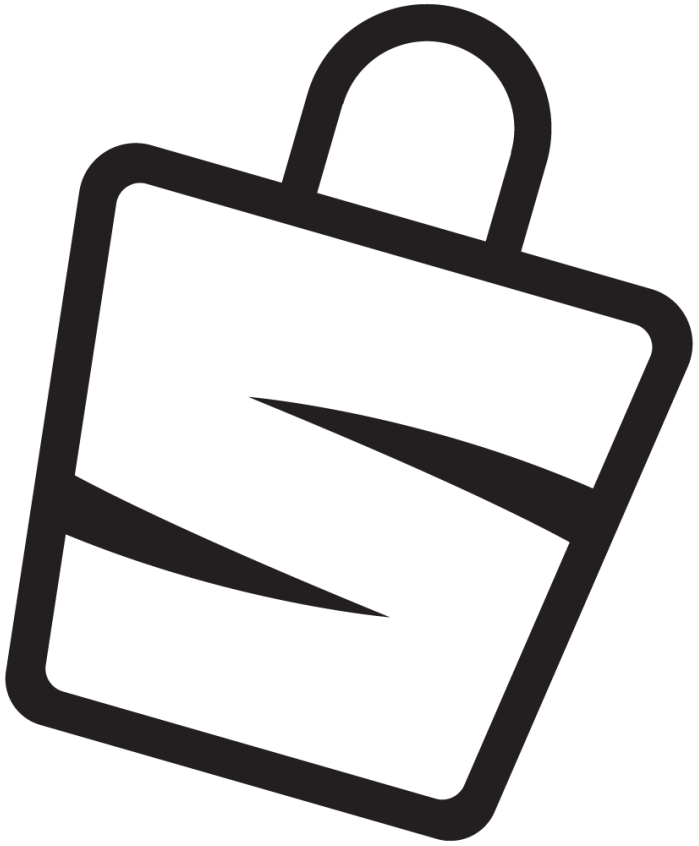

General Data Protection Regulation

Revision 0.4, April 2018

1 Introduction

25th of May 2018, the General Data Protection Regulation (GDPR) will be enforced resulting in stringent regulations concerning the processing and protection of personal data. This document contains all the information about Sellify and these regulations.

This document starts by focussing on the regulations that are applicable to Sellify. Following is a chapter about the organizational and technical measures installed to meet the high protection levels and standards required by the GDPR.

Afterwards, Data Governance is covered (both Client and Data Subject oriented), which forms an essential part of the GDPR. This chapter also presents the required, but out-of-the-box, solutions that we provide our clients and their customers. This document ends by providing relevant information about Sellify, including disclaimers and contact information.

In summary: This document should provide you with a clear understanding of all GDPR-related matters and the steps Sellify has taken to comply to them. When possible, we refer to specific articles found in the GDPR.

It is highly recommended to read the document "Privacy Policy" in advance. This document provides detailed information about Sellify's Data Processing and all the Personal Data that is processed.

1.1 Document history

0.1	2018-01-01	Initial concept document
0.2	2018-03-10	Updated security (concept)
0.3	2018-03-15	Minor changes (concept)
0.4	2018-04-18	In review
0.5	Expected	

2 General Data Protection Regulations

2.1 Data processor

Sellify qualifies as a Data Processor and should, therefore, comply to all the regulations concerning Data Processors.

2.2 Service Agreement (Article 28)

Attached to this document there is a Service Agreement Template that forms an integral part of all commercial and legal contracts in place between Sellify and our Clients, see Appendix: Service Agreement Template .

2.3 Explicit Instructions (Article 29)

Sellify requires the **explicit instructions** from the Client for any Data Processing, unless required to do so by Union or Member State Law. Without this consent, Sellify won't offer its services and can't be held responsible for any claim and/or damage.

This requirement is enforced in the Service Agreement, see the appendix of this document.

2.4 Client supervisory powers

The Client is not only entitled, but encouraged by Sellify, to carry out inspections, either by themselves or with any approved external auditor. This has the sole purpose of ensuring compliance with this Service Agreement in business operations. These inspections should primarily target the verification of " 4. Technical and Organizational Measures ."

Such inspections should be communicated to Sellify in advance in written form (i.e., email) with at least a two week notice. Sellify ensures that the Client can verify compliance with the obligations as set out in Article 28 GDPR.

These inspections should align and not impact Sellify's general way of working

2.5 Personal Data Breach (Article 33 & 34)

Sellify complies with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments, and prior consultations, as referred to in Articles 32 - 36 with the installment of the following measures and precautions:

When Sellify detects or suspects a (personal) data breach it will notify the Client no later than 72 hours after such detection or suspicion. Each notification will include:

1. The nature of the data breach
2. Contact details of the Data Protection Officer
3. Consequences (if any) of the data breach
4. Measures to be taken to mitigate

Sellify ensures an appropriate level of (data) protection through 3.2 Technical and Organization Measures. Next to that, Sellify offers the Client full support with regard to prior consultation of any supervisory authority.

2.6 Data Protection Officer (Article 37, 38, 39)

Sellify has a designated a Data Protection Officer that fully complies to Articles 37 - 39. You can find contact details at: 5.3 Data Protection Officer.

Sellify's Data Protection Officer is involved with all issues and measures that relate to security and is aware of all software designs and implementations. The Data Protection Officer has direct access to the code base and can perform independent checks and verifications.

Next to our designated Data Protection Officer, we have a Chief Security Officer, who can provide all ins and outs of our (technical) security measures. You can find his contact details at the end of this document.

2.7 Codes of Conduct (Article 40, 41)

Not available at the moment. To be expected around Q1 2018.

2.8 Certification (Article 42, 43)

1. Our infrastructure / hosting is ISO 27001, ISO 9001, PCI-DSS, NEN 7510, and ISAE 3402 certified.

2.9 Transfers of personal data (Article 44, 45)

Sellify's headquarters is in Amsterdam, the Netherlands. We're registered under the Dutch Law and are not considered - nor made part of - an international organization. Therefore, we don't apply to the regulations discussed in Chapter V.

Sellify ensures that its processing of data is carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every Transfer of Data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of the Client and shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled.

Chapter V of the GDPR clearly states that when international organizations are involved, the regulations of Chapter V apply. In order to comply to these regulations, Sellify requires a waiver (embedded in the Service Agreement Template) ensuring that the Client - only when considered an international organization - ensures adequate levels of (data) protection (Article 45).

3 Technical and Organizational Measures

Sellify has installed numerous technical and organizational measures r to ensure an appropriate level of (data) protection. These measures include:

1. Taking the circumstances and purposes of the processing into account, as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities.
2. Enabling an immediate detection of relevant infringements events.

3.1 Privacy By Design and by Default (Article 25)

Sellify considers data privacy on the onset of all projects, products, product development, and Services offered, never as an afterthought. Sellify's Data Protection Officer is involved in all issues, measures, and (software) designs that relate to security and has independent and direct access to all source code.

3.2 Technical Measures

Technical measures are divided into various subsections, each of them separately discussed.

3.2.1 Security

1. Employee related:
    a. All workstations (laptops & desktops) of employees are encrypted using disk encryption.
    b. Access to various web applications accessible by employees are using single-sign-on using two-factor authentication (Google Oauth) and require Virtual Private Network (VPN) when working remotely.
    c. Administrator access to Sellify Platform Management interface is only allowed by VPN.

2. Production environment related:
    a. Logging in to the servers is only possible by means of public / private key exchange, passwords are not used.
    b. Administration panel requires two factor authentication.
    c. All security updates are automatically installed and the server is always up-to-date.
    d. Strict firewall configuration from the public internet that only allows HTTP and HTTPS access on load balancers.
    e. Communications to and from the servers, as well as backups, are only performed via secured channels (SSL / HTTPS).
    f. There is active monitoring (graylog + alerts) and banning of incorrect login attempts (fail2ban).
    g. All (virtual) servers are hosted externally.

3. About Personal Data:
    a. All data is pseudonymised.
    b. All personal data is kept using a retention period
    c. Graylog required for system monitoring has a retention period of 30 days max.
    d. Backup data is stored in proprietary binary format (“*pseudo encrypted”*) separated per client.

3.2.2 Hosting & Infrastructure

Sellify hosts its complete infrastructure at AWS and is ISO 27001, ISO 9001, PCI-DSS, NEN 7510, and ISAE 3402 certified.

All of our (virtual) servers and all of our data storage is located within the European Union. This includes our backup copies stored in Amazon Web Services S3 (AWS), whose designated location is in Frankfurt.

3.3 Organizational Measures

3.3.1 Security

We have the following organizational measures in place concerning security:

1. Code-review is required for all software that communicates with the Database.
2. Use of a development model for software that works with small updates on each occasion to minimize the security impact of the updates.
3. Only the employees who must maintain the Database server have access.
4. Audit-logging of all attempts to login into the Database server.
5. Employees cannot physically access the servers.
6. All employees are obliged to maintain confidentiality (see 3.3.2. Confidentiality)

3.3.2 Confidentiality

All employees of Sellify have signed an explicit clause in their employment contract that enforces confidentiality during the employment contract as well as thereafter - regardless of the manner in which and the reasons for which the employment contract has ended - to refrain from making any statement to third parties, in any way, directly or indirectly, or in any form, about data of a confidential nature in connection with the business of Sellify and/or businesses affiliated with it.

3.3.3 Subcontracting

Sellify does not work with any subcontractors that provide services that relate directly to the provision of the principal services as described in this document.

Concerning ancillary and auxiliary services provided by third parties (e.g. telecom, hosting), when possible, Sellify makes appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even when such services are outsourced.

3.3.4 Disaster Recovery

Sellify has disaster recovery (DR) procedures, policies, and scripts defined and in place.

3.3.5 Segregation of Duty (SoD)

The basic concept underlying segregation of duties is that no employee or group should be in a position to perpetrate or conceal errors or fraud in the normal course of their duties. In general, the principal incompatible duties to be segregated are:

- Authorization or approval of related transactions affecting those assets
- Custody of asset
- Recording or reporting of related transactions

The importance of SoD arises from the consideration that giving a single individual complete control of a process or an asset can expose the organization to risk. Principally, several approaches are optionally viable as partially or entirely different paradigms:

- Sequential separation (two signatures principle)
- Individual separation (four eyes principle)
- Spatial separation (separate action in separate locations)
- Factorial separation (several factors contribute to completion)

3.4 Penetration Tests (Article 35)

As part of the Data Protection Impact Assessment (Article 35), Sellify is regularly subject to *penetration tests* (i.e. Pentests) executed by a Client, a (Data) Controller or a designated external and objective party capable thereof.

Pentests are primarily done at the request of the Client but also might be initialized by ourselves, especially after major changes and/or upgrades. The results of the pentests authorized by ourselves - whenever available - might be made publicly available or sent to a Client upon written request.

Pentests are part of Data Protection Impact Assessment (Article 35)

3.5 Bug Bounty Programs

We have continuous testing process in place, and want to scale this up by becoming a member of Hackerone in Q4 2018. See: https://www.hackerone.com/.

“HackerOne Response is a solution for organizations to receive and manage security vulnerability reports from external third parties. Designed to be compliant with responsible disclosure best-practices as recommended and mandated by industry associations and government entities, HackerOne Response reduces the risk of critical security disclosures surfacing on unauthorized channels by giving your team the visibility and tools they need to take action.”

3.6 Quality Assurance

Sellify complies with the statutory requirements referred to in Articles 28 to 33. Accordingly, Sellify ensures compliance with the following requirements:

1. Sellify has designated a Data Protection Officer. See 5.3. Data Protection Officer for contact details.
2. Sellify ensures an appropriate level of (data) protection through 3. Technical and Organization Measures.
3. Sellify offers Client full support with regard to prior consultation of any supervisory authority.
4. Sellify periodically - at least once a year - checks its internal processes and the Technical and Organizational measures to ensure that its services and data processing complies to all requirements of applicable data protection law and the protection of the rights of the Data Subject.
5. The Client is entitled to verify the quality assurance of the services provided by Sellify to ensure quality control.

4 Data Governance

4.1 Client Data Governance

4.1.1 Copies & Duplication

Copies and/or duplicates of the Client's data shall never be created without explicit request and written approval of the Client, the following exceptions are taken into account:

1. Backup copies as far as they are necessary to ensure a continuous service
2. Data required to meet regulatory requirements (for retaining data)

4.1.2 Termination

Not later than 8 weeks after termination of the Services between Sellify and Client, or earlier upon explicit written request by Client, Sellify shall delete any data that is collected, constructed, or generated by any service provided by Sellify as described in this document.

This includes:

1. All documents
2. All collected data
3. All backup data
4. All constructed data (including insights)

Documentation that is used to demonstrate orderly data processing in accordance with this Service Agreement shall be stored beyond the contract duration, respective retention periods are taken into account. Sellify might hand-over this documentation to the Client in order to relieve its contractual obligation.

In the case of deletion, Sellify shall provide the Client evidence by handing over a log of all deleted material. Additionally, the Client might request an inspection to validate that all its data is removed accordingly.

Deletion of Client Data includes all Personal Data of all Data Subjects belonging to Client. Trivially this results in no more access, correction, or data portability for any Data Subject since all their data is deleted.

4.1.3 Backup Copies

All backup files are stored in a highly secured digital environment (Amazon AWS), only accessible by Sellify employees using private keys over SSL.

4.1.4 Export

Sellify offers Client data export functionality of data collected and/or processed by Sellify. Data will be provided in a CSV format and only send to the admin email after verified password authentication.

4.2 Personal Data Governance

As part of the GPPR, Data Subjects (i.e., natural persons or website visitors in our context) can manage their personal data collected and/or constructed by Sellify Services through the Client's website.

4.2.1 Consent (Article 6,7,8)

As required by GDPR, Data Subjects are required to provide explicit consent to any data processing related activities, see article 6 and 7 of GDPR.

It's the obligation of the Controller and/or Client to take care of this regulation and get Data Subject's consent. Sellify will provide access to its privacy policy when someone is interacting with our service.

Keep in mind that whenever a Data Subject is less that 16 years old, additional regulations apply (Article 8).

4.2.2 Right to Rectification (Article 16)

Part of the GPPR is the right for each Data Subject to alter, adjust, or correct their Personal Data. At the current time of writing, it is unclear if this right only affects information provided *directly* by the Data Subject or not.

From a compliance perspective, it is impossible for Sellify to provide the Data Subject a means to change all constructed and aggregated information - i.e., Personal Data - that is *not directly* provided by the Data Subject; this would interfere and corrupt the integrity of all data, its logical processing, and disrupt up reporting. Therefore, we've decided to only focus on providing functionality to modify Personal Data directly provided by the Data Subject.

Requests for altering data can be send per email and is provided in our Privacy Policy

4.2.3 Right to Erasure (Article 17)

By means of our Privacy Policy individuals can email *a* delete request to delete and remove all their personal data. Due to obligations as set forth in the GDPR and law, backup copies are not affected. However, blacklists are carefully maintained containing all user ids that are deleted, so that whenever a (disaster) recovery takes place, information belonging to deleted profiles is not ignored and, thus, not restored.

Sellify has taken the following - technical and organizational - measures into account for when a Data Subject requests their data to be deleted:

1. Our primary store of record is given the nature of storing and processing big data constructed as "write append," making it impossible to "truly" delete data. In order to delete personal data, we ensure that:

    A. All records belonging to given Data Subject as marked as deleted.
    B. Replace all personal data (e.g. column fields) with either zeros or blank values

2. When data is deleted, Sellify provides proof by handing over a log of all data deleted when available (Article 19).
3. System data (including system & activity logs) can't be deleted. However, these data is only kept for limited period (max 30 days).

4.2.4 Right to Restriction of Profiling (a.k.a. Opt-out) (Article 18)

Sellify has a limited impact. We only store data when interacted with our service. Opt-out is always an option provided in our privacy statement.

4.2.5 Right to Data Portability (Article 20)

By means of our available Personal Data Portal, Data Subjects can obtain an instant and up-to-date overview of all their personal data at all times. Data will be presented by means of *a CSV file* that is machine readable and widely considered an interoperable format.

That said, we're working on a visual interface (e.g. the Personal Data Portal) that offers the Data Subject a clear overview of all personal data collected and represented in an understable way.

4.2.6 Right to Object (Article 21)

Since, in our case, the right to object and restrict processing are the same, please see 4.2.4 Right to Restriction of Profiling (a.k.a. Opt-out) (Article 18).

4.2.7 Automated individual decision-making (Article 22)

The right to not be subject to a decision based solely on automated processing, including profiling, is identical to the right to restrict processing for Sellify, see 4.2.4 Right to Restriction of Profiling (a.k.a. Opt-out) (Article 18).

After opt-out, the (current & future) processing of Personal Data stops, but the Personal Data will **not** be deleted

4.2.8 Backup of Personal Data

Personal data included in the Client's data that is stored together in an encrypted format and kept in a highly secured digital environment (Amazon AWS) is only accessible by Sellify employees using private keys. Thus, we do not create individual backup copies per Data Subject.

4.2.9 Costs inferred with Data Subject's Rights (Article 12.5)

As clearly stated in the GDPR, all services associated with the personal rights of Data Subjects, i.e., all services found in 4.2 Personal Data Governance, are provided free of charge.

That said, when requests from a Data Subject are manifestly unfounded or excessive, Sellify has the right to charge administrative costs (Article 12.5)

5 Contact Information

5.1 Downloadable content

GDPR https://www.sellify.com/legal/gdpr/
Personal data: https://www.sellify.com/legal/privacy
General Terms: https://www.sellify.com/legal/terms

5.2 Office Address

Sellify (TSH Collab)
Jan van Galenstraat 335
1014 AZ Amsterdam

5.3 Data Protection Officer

Mr. Lennert Pieters
Lennert@sellify.com
+3120 261 5238

5.4 Technical Security Officer

Mr. Joris Pieters
Joris@sellify.com
+3120 261 5238

5.5 Disclaimers

5.6.1 Compensation

Sellify might charge compensation for support services which are not included in this Service Agreement and/or are not attributable to failures on behalf of Sellify.

5.6.2 Governing Law and Jurisdiction

Services provided by Sellify, including our Service Agreements, are exclusively governed by the laws of the Netherlands. All disputes arising in connection with a Service Agreement, or further agreements resulting thereof, shall (in first instance) exclusively be settled by the competent court of Amsterdam, the Netherlands.

6 Appendix: Service Agreement Template

See: XXX