silverfin

Silverfin Data Processing Agreement

Version February 2021

GENERAL

Parties seek to implement a data processing agreement that complies with the requirements of the governing Data Protection Law, including the GDPR. Unless otherwise agreed in writing, this Silverfin Data Processing Agreement, including its Schedules (the "Agreement") supplements the Silverfin SaaS agreement concluded between Silverfin and the Customer (the "SaaS Agreement") and is entered into by and between the latter Parties.

Pursuant to the SaaS Agreement, Silverfin provides the Silverfin platform (the "Platform") to the Customer. In the provisioning of the Platform, Customer Data, including Personal Data is collected and Processed by Silverfin (the "Processor") on behalf of the Customer (the "Controller"). For purposes of this Agreement only, and except where indicated otherwise, the term "Customer" shall include any relevant Participating Affiliate of Customer.

Silverfin evaluates on a systematic basis the impact of the Processing of Personal Data through the use of the Platform. Silverfin implements appropriate technical and organisational measures that meet the requirements taken into account the nature, scope, context and purposes of the Processing through the use of the Platform together with the risk for the rights of natural persons.

This Agreement will supersede and replace all provisions in prior and current agreements between the Parties which relate, directly or indirectly, to the Processing of personal data, privacy, personal data access or data transfer and data security.

If the provisions of the SaaS Agreement contradict or are inconsistent with the provisions of the Agreement, the provisions of this Agreement shall prevail to the extent that the conflict or incompatibility exists.

silverfin

1. DEFINITIONS

1.1. Following terms and expressions are to be defined as follows:

"Affiliate"	means, unless otherwise defined in the SaaS-Agreement, a business entity that directly or indirectly controls, is controlled by or is under common control (the direct or indirect ownership of more than 50% of the voting securities of a business entity) with such Party.
"**Controller**"	means controller as defined in article 4 (7) of the GDPR.
"Customer Data"	means all data in any form Processed by Silverfin on behalf of the Customer for the purposes of delivering the Platform, including, to the extent applicable, Personal Data.
"**Data Protection Law**"	means the GDPR and all other local legislations within the European Economic Area that might be applicable on the Processing of Personal Data.
"**Data Subject**"	means any identified or identifiable natural person to whom the Personal Data relates.
"**GDPR**"	means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
"**Participating Affiliate**"	means an Affiliate of Customer that: has not entered into a separate SaaS-Agreement with Silverfin and has been authorized to access and use the Service under an existing SaaS-Agreement between Silverfin and Customer.
"**Personal Data**"	means any information relating to an identified or identifiable natural person under the Agreement. 'Identifiable' means a natural person who can be identified directly or indirectly, namely by means of an identifier such as a name, an identification number, location data, an online identifier or by one or more elements which are characteristic for the physical,

	physiological, genetic, psychic, economic, cultural or social identity of that natural person.
"Platform"	means the webbased Silverfin accounting management and reporting platform, including the interfaces which is accessible for Customer..
"**Purposes**"	means the specified, explicit and legitimate purposes of the Processing.
"**Processing**" **or related conjugation of the verb "Process"**	means any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
"**Processor**"	means processor as defined in article 4 (8) of the GDPR.
"Security Incident"	means any unauthorised or unlawful access, deletion, mutilation, loss or any form of unauthorised or unlawful Processing of the Personal Data, or any other incident which shall lead (or may lead) to the accidental or unlawful deletion, loss, modification, unauthorised disclosure of – or access to – the Personal Data, any Personal Data Breach as defined in the GDPR, or any indication that a breach of that nature shall occur or has occurred.
"**Service"**	means Silverfin's online service "Silverfin" including the integrations, features and modules as set out in the SaaS Agreement.

1.2. All terms and expressions as used in this Agreement and which have not been expressly defined herein, will have the same meaning as they have in the SaaS Agreement.

2. DATA PROCESSING

2.1. Parties acknowledge that Silverfin acts as Processor with respect to the Personal Data within the framework of the provision of the Service. In this respect, the Customer is and will remain at all times the Controller with respect to the Personal Data.

2.2. Each Party will comply with its respective obligations under the Data Protection Law with respect to the Processing of Customers' Personal Data.
2.3. The subject-matter of Processing of Personal Data by Silverfin is the performance of the Service pursuant to the SaaS-Agreement. While using the Platform, the Customer may provide certain sets of Personal Data including Personal Data to Silverfin for Processing. Silverfin will only Process Personal Data during the term of the SaaS Agreement or alternative duration to be agreed upon, which as the case may be upon early termination and will in no event keep Personal Data longer than required for the purposes for which they are Processed.
2.4. The nature and purpose of the Processing, the types of Customers' Personal Data and categories of Data Subjects Processed under this Agreement are further specified in Annex 1.
2.5. Personal Data will be primarily processed within the European Economic Area. Silverfin shall be entitled to transfer Personal Data to countries outside the European Economic Area provided that such transfer is done in accordance with the applicable Data Protection Law regarding additional safeguards.

3. OBLIGATIONS AND INSTRUCTIONS OF THE CUSTOMER

3.1. By entering into this Agreement, Customer instructs Silverfin to Process Customer Personal Data: (a) to provide the Service in accordance with the features and functionality of the Service; (b) to enable Customer's and Authorized User initiated actions on and through the Service; (c) as set forth in this Agreement and/or the SaaS-Agreement; and (d) as further documented by prior written instructions given by Customer (e.g. e-mail). Parties agree that the aforementioned sets out Customer's complete and final processing instructions.
3.2. Silverfin shall inform Customer if, in its opinion, Customer's instruction infringes the GDPR or other Data Protection Law. Upon providing such notification, Silverfin will be entitled to suspend performance of such instruction and to no further continue to Process the Personal Data in accordance with previously provided instructions. The Customer shall not be entitled to any indemnity or damages for such stay in performance.
3.3. If Silverfin is required to Process or transfer Personal Data to a third country or an international organization, by Union or Member State law to which it is subject to, Silverfin will inform the Customer of that requirement, unless that law prohibits such information.

3.4. Within the scope of this Agreement and in its use of the Service, Customer shall be responsible for complying with all requirements that apply to it under the applicable Data Protection Laws with respect to its Processing of Personal Data.

3.5. In particular but without prejudice to the generality of the foregoing, Customer acknowledges and agrees that it shall be solely responsible for: (i) the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under the applicable Data Protection Laws for the collection and use of the Personal Data; (iii) ensuring it has the right to transfer, or provide access to, the Personal Data to Silverfin for Processing in accordance with the terms of the Agreement; (iv) ensuring that its instructions to Silverfin regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws. The Customer shall inform Silverfin without undue delay if it is not able to comply with its responsibilities under this subsection or applicable Data Protection Laws.

3.6. No provision of this Agreement includes the right to, and Customer shall not, directly or indirectly, enable any person or entity other than Authorized Users to access and use the Service or use (or permit others to use) the Service other than as described in the SaaS-Agreement and/or this Agreement, or for any unlawful purpose.

4. CONFIDENTIALITY

4.1. Silverfin undertakes to guarantee the confidentiality of the Personal Data Processed.

4.2. Silverfin shall inform any person, including but not limited to employees, interim staff or self-employed workers, who has access to the Personal Data of the obligations on behalf of Silverfin with regard to the Customer's Personal Data.

4.3. Silverfin shall make sure that all persons involved in the Processing of the Customer's Personal Data are subject to professional or statutory obligations of confidentiality, with the purpose of safeguarding the confidentiality and integrity of the Customer's Personal Data.

5. TECHNICAL AND ORGANISATION MEASURES

5.1. Silverfin has implemented appropriate technical and organisational measures as set forth in Annex 2 to ensure that Processing is performed in accordance with the Data Protection Law, to ensure an appropriate level of security of the Personal Data, taking into account the state of the art, the costs of implementation and the

nature, scope, context and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

5.2. The Customer confirms that, based on Customer's risk assessment, it approves the security measures undertaken by Silverfin as set forth in Annex 2.

5.3. The Customer acknowledges that security requirements are changing continually, and that effective security requires a frequent assessment and regular improvement of security measures. Silverfin shall therefore continually assess and tighten, supplement or improve the measures implemented for the continued compliance with its obligations. Silverfin may modify or update the technical and organisational measures at its sole discretion provided that such modification or update does not result in a material degradation in the protection offered by the current measures.

5.4. Silverfin will document all information necessary in order to demonstrate the above mentioned compliance (including records of processing activities). Silverfin may make this documentation available to Customer upon its request.

5.5. The provisions under this Section constitutes an obligation for Silverfin to use its best endeavors.

6. SUB-PROCESSORS

6.1. Customer authorizes to use third party sub-processors to Process (and transfers) Personal Data on its behalf.

6.2. Silverfin has currently appointed, as sub processors, its Affiliates and third parties as listed in Annex 3. Upon execution of this Agreement, Customer explicitly gives its written authorization to engage those sub-processors to Process Personal Data on Customer's behalf.

6.3. Silverfin shall notify Customer by email and/or by notification on the Platform of any intended changes concerning the addition or replacement of its current sub-processors **prior** to any such changes. The Customer will be allowed to object to such addition or replacement on reasonable grounds relating to the protection of Personal Data within 30 days after the notification by submitting by email to legal@silverfin.com. The Customer's failure to object within this timeframe shall be deemed to have waived its right to object and to have authorized Silverfin to engage such sub-processor.

6.4. If Customer does notify Silverfin of such an objection, Parties will discuss Customer's concerns with a view to achieving a reasonable resolution. If no such resolution can be reached, Silverfin will, at its sole discretion, either not appoint the new sub-processor, or permit Customer to suspend or terminate the affected Service in accordance with the termination provisions of the SaaS-Agreement

without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination of the SaaS-Agreement).

6.5. Silverfin's sub-processors will be held to the same contractual obligations as set out in this Agreement to the extent applicable to the nature of the services provided by such sub-processors. Where a sub-processor fails to fulfil its data protection obligations, Silverfin will remain fully liable towards the Customer for the performance of that sub-processor's obligations.

7. INFORMATION OBLIGATIONS AND ASSISTANCE

7.1. Taken into account the nature of the Processing, Silverfin shall, assist the Customer for the fulfilment of its obligation to respond to requests for exercising the Data Subject's rights by:

(i) promptly notifying the Customer if it receives a request from a Data Subject, the Supervisory Authority and/or other competent authority under any applicable Data Protection Laws with respect to Customer's Personal Data;

(ii) by appropriate technical and organizational measures, insofar as this is possible, and provide its reasonable cooperation to the Customer in order to respond to requests for exercising the Data Subject's rights in accordance with the GDPR, after having obtained the approval from and having been instructed by the Customer.

(iii) by ensuring that Silverfin has the technical and organisational capabilities to remove from its system, records or databases and deleting, within a 30-days period, any Personal Data of the Data Subject requesting such a right. Personal Data may persist on backup or archival media which shall be securely isolated and protected from any further Processing and shall be definitely removed in accordance with its retention policy.

Notwithstanding the foregoing, the Customer remains responsible for compliance of such Data Subject requests.

7.2. Silverfin will assist Customer in ensuring compliance with the obligations related to the security of Personal Data and of Processing, taking into account the nature of the Processing:

(i) Silverfin keeps the Customer's Personal Data logically separate from any data belonging to Silverfin and/or third parties, ensuring that the Customer's Personal Data is under no circumstances combined or mixed with any other data;

(ii) Silverfin has implemented a two-factor or multi-factor authentication for the access of the Platform by the Customer;
(iii) Silverfin ensures the ongoing confidentiality, integrity, availability and resilience of the Platform;
(iv) Silverfin has the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident.

7.3. Taking into account the nature of Processing and to the extent that the required information is reasonably available to Silverfin (and Customer does not otherwise have access to the required information), Silverfin shall upon request, provide reasonable assistance to the Customer with the execution of a data protection impact assessment (DPIA) and possible prior consultation with competent supervisory authorities. To the extent permitted by applicable Data Protection Law, Customer shall be responsible for any costs arising from Silverfin's provision of such assistance.

7.4. Silverfin shall notify the Customer by email and without undue delay and within 48 hours after becoming aware of a Security Incident. Customer shall ensure that its contact information is current and accurate at all times during the terms of this Agreement. Silverfin shall make reasonable efforts to identify the cause of such personal data breach and take those steps as Silverfin deems necessary and reasonable in order to remediate the cause of such personal data breach to the extent the remediation is within Silverfin's reasonable control.

Silverfin shall provide the Customer with the following information (to the extent known) relating to the Security Incident:

- the nature of the Security Incident,
- the categories of Data Subject(s), where possible,
- the estimated number of Data Subject(s) imposed to the breach,
- the categories of Personal Data,
- the estimated number of affected Personal Data,
- the name and contact details of the data protection officer, or in the absence the privacy officer, or any other contact point where more information about the personal data breach can be obtained,
- the likely effects and risks, including the likely effects and risks for the Data Subjects,
- he measures taken to handle the Security Incidents, including, where appropriate, measures to mitigate any adverse effects and risks.

If required by Data Protection Law, the Customer will notify the data breach to the supervisory authority and the affected Data Subjects. Silverfin will assist the

Customer in this respect if this is deemed necessary by the latter. To the extent permitted by applicable Data Protection Law, Customer shall not be allowed to refer to Silverfin in any public press releases associated with the Security Incident without Silverfin's prior consent.

Silverfin's notification of or response to a Security Incident under this Section will not constitute an acknowledgment of fault or liability with respect to the Security Incident, and the obligations herein shall not apply to Security Incidents that are caused by Customer or its Authorized Users.

7.5. Silverfin shall make available to Customer all information necessary and to the extent as requested by law to demonstrate compliance with the obligations laid down in this Agreement and allow for and contribute to audits, including inspections, conducted by an external auditor mandated by Customer during the term to ensure compliance with the terms of the Agreement.

7.5.1. However, the Customer will limit his initiatives to perform an audit or an inspection to a maximum of once a year except in case (i) it is legally imposed, (ii) Silverfin has experienced a Security Breach within the prior twelve (12) months which has impacted your Customer Personal Data or (iii) of a mutual agreement, and must notify Silverfin at least 30 working days in advance. All audit costs are exclusively borne by the Customer, except in case of a severe security incident or data breach where the Customer will be entitled to a free audit to ensure all necessary and agreed actions have been taken by Silverfin to mitigate any recurrence. In that case, Silverfin reserves the right to mandate an independent auditor to conduct the audit on its behalf.

7.5.2. The Customer shall guarantee that the audit is carried out in such a way that the inconvenience for Silverfin is kept to a minimum. The Customer will impose sufficient confidentiality obligations on its auditors. In addition, Silverfin has the right to require from the Customer and its auditors to sign a non-disclosure agreement before the start of the audit.

7.5.3. Silverfin may limit the access of the Customer to the premises of Silverfin to a space provided by Silverfin and the auditor may not copy or delete documents from Silverfin without the prior approval and consent of Silverfin.

7.5.4. The scope of any audit shall not require us to disclose to the auditor, or to allow the auditor to access: a) any data or information of any other Silverfin customer; b) any Silverfin internal accounting or financial information; c) any Silverfin trade secret or information related hereto; d) any information that, in our reasonable opinion could compromise the security of our systems or

premises or cause us to breach our obligations under Data Protection Law or our security, confidentiality and or privacy obligations to any other Silverfin customers or any third party; or e) any information that auditor seek to access for any reason other than the good faith fulfilment of the obligations under the Data Protection Law and our compliance with the terms of this Agreement.

7.5.5. If Silverfin declines or is unable to follow the instructions regarding audits permitted under this Section, the Customer will be entitled to terminate this Agreement for convenience.

8. DELETION OR RETURN

8.1. Silverfin will delete or return all Personal Data (as well copies thereof) Processed pursuant to this Agreement, on termination or expiration of the SaaS Agreement, except that this requirement shall not apply to (i) if Silverfin is required by applicable law to retain Personal Data or (ii) Personal Data it has archived on back-up systems, which data Silverfin shall securely isolate and protect from any further Processing and shall be deleted in accordance with its retention policy.

8.2. The Customer shall inform Silverfin of their request to delete or return the Personal Data within 30 days after the SaaS-agreement has been terminated or expired by sending a request to (legal@silverfin.com). Silverfin shall confirm to the Customer that the deletion has been completed within an agreed timescale by sending a confirmation email. Without further notice from the Customer within 30 days, Silverfin will delete your account, including your Personal Data in order to comply with our retention data policy.

9. TERM

9.1. This Agreement will terminate automatically upon termination of the SaaS-Agreement or as earlier terminated pursuant to the terms of this Agreement.

10. LIMITATIONS OF LIABILITY

10.1. Nothing in this Agreement shall limit or exclude any liability, rights or remedies provided by law towards the data subject who suffered damage as a result of an infringement of GDPR caused by Silverfin in its capacity as Processor.

10.2. Each party shall on their own be liable for any administrative fines that the supervising authority impose due to their own Processing.

10.3. In case of a proven breach by Silverfin of its obligations under this DPA or under the GDPR, Silverfin shall be liable for the proven direct damages incurred by the

Customer. Silverfin shall not be liable for indirect, immaterial and/or consequential damages, including loss of profit, loss of opportunities, loss of and/or damage to data, loss of reputation, sanctions and/or fines, and unforeseeable damages. Silverfin's liability towards Customer shall in any case be limited to the total amount paid by Customer to Silverfin during the last 12 months under the SaaS Agreement.

10.4. The provisions in this Section shall be without prejudices to any other liabilities as agreed upon in the SaaS-agreement.

11. GOVERNING LAW AND JURISDICTION

11.1. This Agreement will be governed by and construed in accordance with governing Data Protection law of Belgium, unless required otherwise by applicable Data Protection Laws. Any disputes arising out of this Agreement shall be settled by the courts of the arrondissement of Ghent, division of Ghent.

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement as of the Effective Date.

For Silverfin NV	For the Customer
Name: YELLOWFIN VENTURES BV represented by Joris Van Der Gucht permanent representative	Name:
Title: Managing director	Title:
Date:	Date:
Signature:	Signature:

silverfin

Annex 1 – Data Processing

Type of Personal Data	Category of Data Subject	Nature of Processing Carried Out	Purpose(s) of Processing	Duration of Processing
Name, surname, residence address	Clients of Data Controller Employees of (clients) of Data Controller Shareholders of (clients) of Data Controller Directors of (clients) of Data Controller Suppliers of (clients) of Data Controller Customers of (clients) of Data Controller	collecting, sorting, structuring, modifying, saving, transferring, consultation, comparison, interconnection, communicating, restricting and deleting data	Providing of services pursuant to the SaaS Agreement	Term of the SaaS Agreement
Financial data:	Clients of Data Controller Employees of (clients) of Data Controller Shareholders of (clients) of Data Controller Directors of (clients) of Data Controller Suppliers of (clients) of Data Controller Customers of (clients) of Data Controller	collecting, sorting, structuring, modifying, saving, transferring, consultation, comparison, interconnection, communicating, restricting and deleting data	Providing of services pursuant to the SaaS Agreement	Term of the SaaS Agreement
Email addresses	Clients of Data Controller Employees of (clients) of Data Controller Shareholders of (clients) of Data Controller Directors of (clients) of Data Controller	collecting, sorting, structuring, modifying, saving, transferring, consultation, comparison, interconnection, communicating,	Providing of services pursuant to the SaaS Agreement	Term of the SaaS Agreement

	Suppliers of (clients) of Data Controller Customers of (clients) of Data Controller	restricting and deleting data		
Telephone numbers	Clients of Data Controller Employees of (clients) of Data Controller Shareholders of (clients) of Data Controller Directors of (clients) of Data Controller Suppliers of (clients) of Data Controller Customers of (clients) of Data Controller	collecting, sorting, structuring, modifying, saving, transferring, consultation, comparison, interconnection, communicating, restricting and deleting data	Providing of services pursuant to the SaaS Agreement	Term of the SaaS Agreement
Any other personal data filled in by a user of the software in a free form field	Clients of Data Controller Employees of (clients) of Data Controller Shareholders of (clients) of Data Controller Directors of (clients) of Data Controller Suppliers of (clients) of Data Controller Customers of (clients) of Data Controller	collecting, sorting, structuring, modifying, saving, transferring, consultation, comparison, interconnection, communicating, restricting and deleting data	Providing of services pursuant to the SaaS Agreement	Term of the SaaS Agreement
Electronic identification data (IP address, log in data, usage data, browser data cookies, geolocation information,	Authorized Users	Interconnection and communicating	Providing of services pursuant to the SaaS Agreement	Term of the SaaS Agreement

passwords, analytic data ...)				

silverfin

Annex 2 – Technical and organisational measures

A. *Management Direction for Information Security*

i. Silverfin has implemented an appropriate information security policy.

ii. Silverfin has suitably qualified information security specialists, supported by the Silverfin business leadership.

iii. Silverfin management requires employees and third-party contractors with access to Customer information to commit to written, confidentiality, and privacy responsibilities with respect to that information. These responsibilities survive termination or change of employment or engagement.

B. *Human Resource Security*

i. Silverfin provides information security awareness information to employees and relevant third-party contractors.

C. *Access Control*

User Access Management

i. Silverfin implements access control policies to support creation, amendment and deletion of user accounts for systems or applications holding or allowing access to Customer information.

ii. Silverfin implements a user account and access provisioning process to assign and revoke access rights to systems and applications.

iii. The use of “generic” or “shared” accounts is prohibited without system controls enabled to track specific user access and prevent shared passwords.

iv. Silverfin monitors and restricts access to utilities capable of overriding system or application security controls.

v. User access to systems and applications storing or allowing access to Customer information is controlled by a secure logon procedure.

Physical Access Management

vi. Physical access to facilities where Customer information is stored or processed is protected in accordance with good industry practices

D. *Communications Security*

Network Security

i. Silverfin logically segregates Customer data within a shared service environment.

ii. Silverfin secures network segments from external entry points where Customer data is accessible.

iii. External network perimeters are hardened and configured to prevent unauthorized traffic.

iv. Inbound and outbound points are protected by firewalls and intrusion detection systems (IDS). c. Ports and protocols are limited to those with specific business purpose.

v. Silverfin synchronizes system clocks on network servers to a universal time source (e.g. UTC) or network time protocol (NTP).

Cryptographic Controls

vi. Customer data, including personal data, is encrypted at rest.

Cloud Controls

vii. Silverfin encrypts data during transmission between each application tier and between interfacing applications.

E. Operations Security

Service Management

i. Silverfin has implemented formal operating procedures for system processes impacting Customer data. This notification may occur through generic change logs. Procedures must track author, revision date and version number, and must be approved by management.

ii. Silverfin monitors service availability.

Vulnerability Management

iii. Silverfin performs annual penetration testing for systems and applications that store or allow access to Customer data, including personal data. Identified issues must be remediated within a reasonable timeframe.

iv. Silverfin has implemented a patch and vulnerability management process to identify, report and remediate vulnerabilities by:

a. Implementing vendor patches or fixes.

b. Developing a remediation plan for critical vulnerabilities.

v. Silverfin has implemented controls to detect and prevent malware, malicious code and unauthorised execution of code. Controls must be

updated regularly with the latest technology available (e.g. deploying the latest signatures and definitions).

F. Logging and Monitoring

i. Silverfin generates administrator and event logs for systems and applications that store or allow access to Customer data.

ii. Silverfin reviews system logs periodically to identify system failures, faults, or potential security incidents affecting Customer information.

G. Third Party Supplier Management

i. Silverfin has contractual agreements with third parties handling Customer information must include appropriate information security, confidentiality, and data protection requirements, as detailed in the Agreement. Agreements with such parties are reviewed periodically to validate that information security and data protection requirements remain appropriate.

ii. Silverfin reviews its third parties' information security controls periodically and validates that these controls remain appropriate according to the risks represented by the third party's handling of Customer information, taking into account any state-of-the-art technology and the costs of implementation.

iii. Silverfin restricts third party access to Customer data, including personal data.

iv. If requested by Customer, Silverfin provides the Customer a list of third parties with required access to Customer data, including personal data.

v. Silverfin permits access to Customer data, including personal data, only as necessary to perform the services that the third party has contractually agreed to deliver.

H. Resilience

i. Silverfin performs business continuity risk assessment activities to determine relevant risks, threats, impacts, likelihood, and required controls and procedures.

ii. Based on risk assessment results, Silverfin documents, implements, annually tests and reviews its Business Continuity and Disaster Recovery (BC/DR) plans to validate the ability to restore availability and access to Customer data in a timely manner, in the event of a physical or technical incident that results in loss or corruption of Customer data.

I. Audit and Compliance

i. Silverfin periodically reviews whether its systems and equipment storing or enabling access to Customer data, including personal data, comply with legal and regulatory requirements and contractual obligations owed to Customer.

ii. Silverfin maintains current independent verification of the effectiveness of its technical and organisational security measures (e.g. ISO certification). The independent information security review are performed at least annually.

silverfin

Annex 3 – Silverfin's sub-processors

Silverfin engages certain sub-processors (including entities within the Silverfin group) to assist it in providing the Services as described in the SaaS-Agreement.

Affiliates

Silverfin Group maintains affiliate companies in countries where Silverfin personnel process Personal Data in order to deliver our Services towards our global Customers.

Name sub-processor	Nature of Processing	Territories
Silverfin Software Ltd.	Support Services	United Kingdom (London)
Silverfin Software B.V.	Support Services	The Netherlands (Amsterdam)
Silverfin Software ApS	Support Services	Denmark (Copenhagen)

Third Party Sub-Processor – Silverfin Platform

Silverfin engages several third-party processors concerning the performance of the Silverfin Platform. Such sub-processors could have access to or process Personal Data by virtue of the services they provide concerning the performance of the Silverfin platform.

Name sub-processor	Nature of Processing	Territories
Fivetran Inc.	Data transfer and integration of data sources	US
Heap Inc.	transmitting, collecting, storing, and analyzing data (including from cookies and device local storage) to provide Customer with analytics information about its visitors' and users' use of its website, mobile applications, and other online services	US
Wildbit, LLC.(Postmarkapp)	Sending mails in connection to the provision of the Silverfin Platform	US

Functional Software, Inc. (Sentry)	Error logging in connection to the provision of the Silverfin Platform	US
Google Ltd	Cloud Infrastructure Hosting Centralized logging in connection to the provision of the Silverfin Platform	EEA
Amazon S3	Storage database's back up	EEA
Datadog Inc.	Infrastructure monitoring	US
Report-URI Ltd.	Security reporting	EEA
Headway App, Inc.	Changelog and communication	US
Conflux VOF	Feedback management	EEA
Delighted LLC	Customer feedback (NPS)	US
Userlane GmbH	Customer onboarding	EEA
Help Scout	Customer onboarding	US

Questions or concerns?

Do you have any questions or concerns? Please contract legal@silverfin.com.