Table of Contents

1. General Notice

1.1. *Introduction.*

Sprinque B.V. (**Sprinque**) is a company based in Amsterdam, the Netherlands, with registered address at Prinsengracht 526-H, 1017 KJ Amsterdam, the Netherlands and registered with the Chamber of Commerce under 81977050. Sprinque is a B2B checkout platform that allows business buyers to make online purchases with the payment terms that best suit their needs, while merchants or marketplaces have the option to get paid instantly for those transactions.

1.2. *Why this privacy statement?*

Whenever you use our services, website, apps or when you correspond with us, whether as our customer (Merchant) or as an End-user of our customers (End-customer) or a visitor to our website: you share (personal) information with us. This statement informs you how and for what purposes we collect, process, store, share and protect your data, for how long we keep your data as well as what rights you have concerning your data.

1.3. *Adherence to GDPR.*

Sprinque is responsible for the data you share with it as a data controller under the General Data Protection Regulation 2016/679 (**GDPR**). It goes without saying that Sprinque adheres to the rules as set forth therein.

2. Collecting, processing and storing your personal data

2.1. ***Information we collect.***

The personal data we collect and the use of such data depend on the context of the business relationship and your interaction with our services, your choices and the services and features you use. Personal data are data relating to an identifiable natural person. Data relating to a company or legal entity (a **Company**) under certain circumstances also qualify as personal data. This is the case in the event of small companies with a sole or few proprietor(s) and/or namegiver(s). Data in relation to contact persons and representatives of a Company also qualify as personal data.

2.2. **Merchant registration.**

2.2.1. When you engage our services, we will ask you to register your Company and provide us with an ultimate beneficial owner declaration, chamber of commerce extract, shareholders register, identity details of authorised representative(s) (i.e. gender, nationality, name, maiden name, date of birth, email, identity document details (ID card, passport, registration certificate)) and evidence that the representative(s) is/are authorised to represent the Company.

2.2.2. This information as well as login information is necessary to create an account, to conduct communication, to evaluate and establish a contractual relationship with the Company and to comply with the Dutch Act on the Prevention of Money Laundering and Terrorist Financing and sanction regulations.

2.2.3. Subsequently we will perform checks with our trusted partners providing us with rating and information services (**Third-party Providers**), to determine whether the Company is trustworthy as our customer in view of our risk and compliance policies. To determine this, we obtain information on corporate identity, ownership, geographical location, payment history and credit default risk.

2.2.4. Furthermore, we perform checks with our Third-party Providers to comply with legislation on the prevention of Money Laundering and Terrorist financing and sanction regulations. For this purpose, we will share the name and, if necessary, birth date and/or nationality of persons associated with the Company to check if they are a so-called politically exposed person or whether they are on a sanctions list. The verification also involves data on law enforcement, insolvency, adverse media and disqualified directors. Depending on the risk assessment, additional information relevant for the specific assessment will be collected and processed. This is done first when the business relationship is established and subsequently on a regular basis. Processing is carried out to comply with the Dutch Act on the Prevention of Money Laundering and Terrorist Financing and sanction regulations

2.2.5. Once a contractual relationship is established, information on the contractual relationship, payment information and correspondence and other communication information is processed to carry out the contractual relationship.

2.2.6. The legal bases for the processing are articles 6.1(b) (i.e. precontractual measures and performance of an agreement), 6.1(c) (i.e. compliance with legal obligation) and 6.1 (f) GDPR (i.e. legitimate interest to mitigate business risks).

2.3. ***End-customers.***

2.3.1. When Merchants offer the option of postponed payment in the purchasing process (**Pay-by-Invoice**) to their End-customers, this is facilitated by us. In order to make this service available, we receive data from Merchants at the time an End-customer creates an account with a Merchant. The following data are collected: name, IP address, address, phone number and email of the End-customer as well as Company name, Chamber of Commerce registration and Company address. Based on these data, we determine whether the End-customer is eligible to use Pay-by-Invoice by conducting fraud and credit checks (see below). We also use these data to improve our services by determining our credit limits and in order to obtain insurance for our services. This processing is based on 6.1(f) (i.e. the legitimate interest of us and of the Merchant) GDPR. It is our legitimate interest to mitigate our credit risk and to improve our risk scoring and fraud detection capabilities. The legitimate interest of the Merchant is to offer the best payment options to End-customers in a responsible way.

2.3.2. When an approved End-customer decides to use Pay-by-Invoice, the Merchant shares transaction information (number and amount of transactions and credit limit) with us in order to check the validity of the transaction and whether the End-customer has credit available within his credit limit. As of that moment we process the End-customer data based on such agreement (article 6.1(b) GDPR).

2.4. ***Credit check.***

When an End-customer creates an account with a Merchant and is eligible for Pay by Invoice, we will share name and if necessary birth date and/or nationality of the representative of the Company as appears from the Chamber of Commerce with our **Third-party Providers** in order to obtain corporate and address information about the Company being registered, as well as data on payment history and credit default risk.

2.5. ***Information on creditworthiness.***

2.5.1. The following information on creditworthiness will be obtained: information on the probability of default using the information on the previous payment history as well as possible ongoing collection or insolvency proceedings or an above-average risk of default based on other risk factors set by our Third-party Providers. If the Company is a legal entity, the processing takes place in an automated way. In respect of companies with a sole or few proprietors that are not legal entities, a separate evaluation by our risk officer will take place. The credit and default risk factors and calculations are further explained in the privacy policies of our Third-party providers which can be obtained by sending a request to founders@sprinque.com

2.5.2. An End-customer may request the human evaluation of the outcome at any time after receipt of a rejection by sending an e-mail to founders@sprinque.com.

2.6. ***Storage period.***

All information is stored for 2 years after the termination of the relationship with a Merchant or End-customer or 1 month after a request for an agreement is rejected, save to the extent a longer storage period is required to comply with financial and tax obligations and legal obligations on the prevention of money laundering. After the retention periods have expired, the data will be stripped of personally identifiable information and only processed in an anonymized form.

2.7. ***Cookies and similar techniques***

When you visit our website, we will collect personal data through the use of cookies and other technologies. Cookies are small data files that are stored on your device through which we store information or from which information may be retrieved by us like IP address, internet browser and device type, location data, the pages you visited, how you got to our website, the time and length of your visit, your language preferences, etcetera. We use cookies and other techniques for our site to technically function, to comply with your preferences. If you provide us with your consent to do so, we also use marketing cookies, functional cookies and/or analytics cookies. . You can find a full list of our cookie nametags, their purposes, third party access and storage periods here: https://support.wix.com/en/article/cookies-and-your-wix-site. You may withdraw your cookie consent at any time on our website, www.sprinque.com. Please note this will not affect any cookies used before withdrawing your consent.

You may also disable cookies through your browser settings. Please note that our website may not always function properly if cookies are disabled through browsersettings.

2.8. ***Email marketing.***

If you have given us your consent to send you information of a promotional nature, such as newsletters or text messages, we will use your e-mail address, postal address and telephone number for the purpose of sending you the relevant information. You can revoke your consent for the future at any time by using the unsubscribe link in the emails sent to you. Such revocation does not affect the lawfulness of the data processing up to that point.

2.9. ***Third parties.***

We only provide your data:

a. To accountants, debt collection agencies, insurance companies and legal advisors;
b. To third-party credit rating providers;
c. To trusted partners who perform the above mentioned checks to comply with anti-money laundering laws and sanction regulations;
d. To parties that act as a processor on our behalf;
e. as part of a merger or acquisition of our company; and
f. as part of a transaction to finance our activities;
g. with your consent or otherwise in accordance with the GDPR.

An accurate list of these third parties is available upon request.

2.10. ***No transfer or storage outside of the EU.***

We store personal data only on servers located within the European Economic Area (EEA).

2.11. ***Security measures.***

We use appropriate, technical, organizational and administrative security measures to protect any information we hold in our records from loss, misuse and unauthorized access, disclosure, alteration and destruction. Among other practices, your account is protected by a password for your privacy and security. You must prevent unauthorized access to your account and personal data by selecting and protecting your password appropriately and limiting

access to your computer or device and browser by signing off after you have finished accessing your account.

3. Rights regarding your data

3.1. ***General.***

You have the following rights regarding your data:

a) *Access.* You may request a written copy of the personal data we hold about you.

b) *Correct.* We want to ensure that your personal data are accurate and current. You may rectify data with us that you believe to be incorrect.

c) *Erase.* You may request us to erase your personal data. If we need the personal data to be able to provide you with our services, we may not be able to erase them immediately. We may not delete information that we are required to keep by law.

d) *Object.* You may object at any time to the processing of your personal data on the basis of article 21 GDPR.

e) *Restrict processing.* You may limit the processing of your data in accordance with article 14 GDPR.

f) *Withdraw consent.* When the processing of your personal data is based on your consent, you have the right to withdraw your consent, without affecting the lawfulness of the processing based on your consent before the withdrawal.

g) *Data portability.* If your personal data are processed by automated decision-making for the fulfillment of our contractual relationship, you have the right to request that we provide you with your personal data in a machine-readable format for transfer to another controller.

h) *Complain.* You may submit a complaint at any time to founders@sprinque.com or to the authority via https://autoriteitpersoonsgegevens.nl/.

i) *Request information.* You may request information about your personal data.

3.2 *E-mail.*

Questions, comments, requests or complaints concerning the processing of your personal data or this privacy statement may be addressed to founders@sprinque.com.

4. Changes in statement

Just as our business is always changing, this Privacy statement may also change from time to time. If we plan to make material changes or changes that have an impact on you, we will always inform you in advance. An example of this kind of change would be if we were to start processing your personal data for purposes that aren't detailed above.