AMENDMENT No. 1

TO THE DATA PROTECTION ADDENDUM

entered into between PagoPA S.p.A. and Instabug, Inc. on March 26, 2020

This Amendment No. 1 ("Amendment") to the above mentioned Data Processing Addendum ("DPA") is effective as of the date of the last signature set forth below (the "Effective Date") by and between Instabug, Inc. (the "Company") and PagoPA S.p.A. (the "Client"), as identified below. All capitalized terms used in this Amendment but not defined herein shall have the meanings ascribed to them in the DPA signed on March 26, 2020

PagoPA S.p.A., with registered office in Piazza Colonna 370, Roma (RM), Italy, VAT number and company's register number 15376371009, represented by Mr. Giuseppe Virgone.

and

Instabug, Inc., with registered office in 855 ElCamino Real, Palo Alto, California, 94302, USA, tax ID 90-0985691, represented by Mr. Omar Gabr.

(hereinafter jointly referred to as "the parties")

WHEREAS the parties have entered into an agreement for the provision of certain services, to which the above mentioned DPA form an integral part.

WHEREAS the parties agreed to stipulate the European Commission's Standard Contractual Clauses (SCCs) exhibited in Annex A of the DPA, in order to regulate data transfers related to said service.

WHEREAS following the Schrems II ruling, the parties have decided to further supplement the SCCs with some additional provisions.

NOW, THEREFORE, in consideration of these premises and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto hereby agree as follows:

1. **Clause 4.4.** of the SCCs exhibited in Annex A of the DPA was mistakenly truncated and is amended as follows to reflect the standard wording issued by the European Commission:

4. That after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

2. **After Appendix 2** of the SCCs exhibited in Annex A of the DPA, the following Appendix 3 is added:

APPENDIX 3

ADDITIONAL SAFEGUARDS TO STANDARD CONTRACTUAL CLAUSES

1. *The data importer will assess whether the laws applicable to it provide adequate protection under European Union ("EU") data protection law. If and to the extent that it determines that any such laws are likely to have a substantial adverse effect on the level of data protection offered by the Standard Contractual Clauses and required under European data protection law, it undertakes to comply with the safeguards set out in paragraphs 2 to 4 below.*

2. The data importer undertakes to adopt supplementary measures to protect the personal data received under the Standard Contractual Clauses from the data exporter ("SCC Personal Data") in accordance with the requirements of EU data protection law, including by implementing appropriate technical and organizational safeguards, such as encryption or similar technologies, access controls or other compensating controls, to protect personal data against any interference

that goes beyond what is necessary in a democratic society to safeguard national security, defence and public security.

3. In the event that the data importer receives a legally binding request for access to the SCC Personal Data by a public authority, it will promptly notify the data exporter of such request to enable the data exporter to intervene and seek relief from such disclosure, unless the data importer is otherwise prohibited from providing such notice, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. If the data importer is so prohibited:

(a) It will use its reasonable best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.

(b) In the event that, despite having used its reasonable best efforts, the data importer is not permitted to notify the data exporter, it will make available on an annual basis general information on the requests it received to the data exporter and/or the competent supervisory authority of the data exporter.

(c) Oppose any such request for access and contest its legal validity to the extent legally permitted under applicable law.

4. In the event of any request for access to the SCC Personal Data by a public authority, the data importer will:

(a) comply with a Data Disclosure Policy, to be provided at request;

(b) not make any disclosures of the SCC Personal Data to any public authority that are determined to be massive, disproportionate and indiscriminate in a manner that it would go beyond what is necessary in a democratic society; and

(c) upon request from the data exporter, provide general information on the requests from public authorities it received in the preceding 12 month period relating to SCC Personal Data.

* * *

IN WITNESS WHEREOF, the parties hereto have caused this Amendment to be duly executed by their respective authorized officers as of the date set forth below.

PagoPA S.p.A.

Giuseppe Virgone

(Amministratore Unico)

Firmato digitalmente da: GIUSEPPE VIRGONE
Ruolo: AMMINISTRATORE UNICO
Organizzazione: PAGOPA S.P.A./15376371009
Data: 01/10/2020 22:39:25

Instabug, Inc.

Omar Gabr

(CEO)