2Checkout Data Processing Agreement "Controller to Processor" version of 16.3.2018

EXHIBIT OF END USER AGREEMENT

Data Processing Agreement
- hereinafter this Agreement –

Content:

1 Preamble

1.1 **2Checkout**, 93 De Cuserstraat, 1081CN Amsterdam, The Netherlands (hereinafter 1.1referred to as the **"Processor"**) distributes via its online shop services, in particular the TestBench Cloud Service as a Service, a specific B2B SaaS service developed, maintained and owned by imbus AG (acting as and hereinafter referred to as "Sub-Processor"), running and made available and hosted on a cloud infrastructure by a third party provider (sub-contractor of the Sub-Processor). The Processor is the Sub-Processor's merchant-of-record and contractual partner of the end user (hereinafter referred to as **"Controller"**) by conclusion of the "End User Agreement" or subscription of TestBench Cloud Service as a Service as well as direct contact person for the Controller. Integral part of the End User Agreement are Service Specifications and Service-Specific Terms and Conditions with regard to the TestBench Cloud Service as a Service. The Processor and the Controller are hereinafter together referred to as the

"Parties".

1.2 To the extent as stated in section 3. of **Attachment 1** to this Agreement, the Sub-Processor has access to and processes the personal data of the Controller commissioned by the Processor. The Processor and the Sub-Processor concluded a Data Sub-Processing Agreement dated 22.1.2018. However, the Processor does not have access and does not collect, use or handle in any way personal data of the Controller which are entered into or uploaded by the Controller within the Sub-Processor's TestBench Cloud Service as a Service.

1.3 This Agreement specifies both Parties' duties with regard to the protection of the Controller's personal data which the Processor processes on behalf of the Controller by engaging the Sub-Processor.

1.4 For the avoidance of doubt, Controller's personal data that are collected in the Processor's online shop is not within the scope of this Agreement as, insofar, the Processor determines the purposes and means of the processing (e.g. handling of payment data).

2 Definitions

2.1 For the purposes of this Agreement

2.1.1 **'Controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; in the context of this Agreement Controller is end customer/" end user" of the Processor.

2.1.2 **'Data'** means any personal data, including special categories of personal data (see sec. 2.1.9) in particular data concerning health (see sec. 2.1.3) of the **Controller** which are object of this Agreement and its Attachments;

2.1.3 **'Data concerning health'** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

2.1.4 **'personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2.1.5 **'personal data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

2.1.6 **'processing'** means any operation or set of operations which is performed on personal data or on sets of 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;

2.1.7 **'Processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller; for the purposes of this Agreement 2Checkout is Processor and imbus AG is the Sub-Processor.

2.1.8 **'pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

2.1.9 **'special categories of personal data'** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

2.1.10 **'third party'** means a natural or legal person, public authority, agency or body other than the data subject, Controller, processor and persons who, under the direct authority of the Controller or Processor, are authorised to process personal data;

3 Object of this Agreement, Term and Termination

3.1 Object of this Agreement are statutory obligations applying to personal data (see definition of "Data" in sec. 2.1.2) of the Controller which, by engaging the Sub-Processor, the Processor processes for the fulfilment of the End User Agreement concluded between the Controller and the Processor and this Agreement by order and on account of the Controller.

3.2 The provisions of this Agreement correspondingly apply where by order the Processor or on his behalf the Sub-Processor do not process Data of the Controller, but where they may have the possibility of authorized access to such Data.

3.3 Determination of the permissibility of any authorized access to Data as stipulated in section 4.1 and the safeguarding of the data subjects' rights is exclusively incumbent upon the Controller.

3.4 The term of this Agreement begins with the effective date of the End User Agreement (subscription of TestBench Cloud Service as a Service) and shall end 30 days after expiration of the subscription unless the subscription is prolonged.

4 Type and Extent of the Processing and access to Controller's Data

4.1 Type and extent of the commissioned data processing for the purpose of providing

TestBench Cloud Service as a Service are described in **Attachment 1**.

4.2 As far as required under the applicable data protection law, in particular Article 28 of the EU General Data Protection Regulation (GDPR), the Controller shall notify whether and to what extent **Attachment 1** needs to be modified or amended regarding type, scope and procedure of the processing as well as categories of Data, in particular special categories of personal data including data concerning health and data subjects. The Controller agrees to provide a corresponding update of **Attachment 1** directly to the Sub-Processor.

4.3 The Processor, by engaging the Sub-Processor, processes the Data for the execution of the End User Agreement with the Controller, specifically for the provision of the TestBench Cloud Service as a Service towards the Controller and not for the Processor's own business purposes. For the sake of clarity, within the Service-Specific Terms and Conditions agreed upon between the Controller and the Processor, the Controller authorizes the Sub-Processor to anonymize Data and use (in particular analyse and aggregate) anonymous data for the Sub-Processor's own business purposes (see also sec. 3.3 of **Attachment 1**).

5 Instructions (including Data Deletion), Data Protection Impact Assessment

5.1 Consistent with the functionality of the TestBench Cloud Service as a Service the Controller is able to delete and correct its Data during the term of the applicable subscription. If the Controller uses TestBench Cloud Service as a Service to delete its Data during the term of the subscription, this Data cannot be recovered by the Controller and this use will constitute an instruction respectively. For any deletion upon termination/expiration of the Controller's applicable subscription resp. the End User Agreement see sec. 3.1 of **Attachment 1**.

5.2 Based on the Controller's explicit instruction, if applicable, the Processor, by means of the Sub-Processor, shall assist in correction, deletion, restriction, and return of respective Data to the Controller as well as Data portability. In cases where a data subject directly approaches the Processor or the Sub-Processor, the Controller agrees and approves that the Sub-Processor and/or Processor shall directly inform the Controller. The Controller's instructions (passed on to the Sub-Processor by the Processor) are limited to legal – both statutory and administrative – requirements of data protection. Such instructions shall be issued in writing (including electronic format).

5.3 The Controller agrees that the Processor or directly the Sub-Processor shall notify the Controller without undue delay in electronic format, if the Processor or Sub-Processor realise that an instruction of a Controller violates applicable data protection law or is more than immaterially defective, incomplete, contradictive or not legally or practically executable. At the same time the Processor shall request from the Controller in electronic format to immediately determine whether the Processor shall nonetheless act upon the instruction at question or whether the Processor shall conduct the processing of Data regardless of the instruction.

5.4 The Controller agrees that where the Controller carries out an assessment of the

impact of the envisaged processing operations on the protection of Data, including such cases where the Controller is involved in prior consultation of the supervisory authority, the Processor shall assist the Controller using reasonable and necessary efforts. The Processor may pass on the request for assistance to the Sub-Processor which will directly assist the Controller. The Processor's assistance is subject to section 12.

6 Information, notification and further obligations

6.1 Any case of more than immaterial personal data breach or reasonable suspicion thereof during the processing of the Data shall be informed to the Controller by either the Processor or directly by the Sub-Processor.

6.2 In case of a personal data breach, the Controller has the responsibility to determine whether he is obliged to notify the personal data breach to the competent supervisory authority and/or to data subjects and to issue respective notifications.

6.3 The Controller may request that the Processor by means of the Sub-Processor provide assistance in gathering the necessary information for the respective notification.

6.4 To the extent permitted by applicable law the Controller shall inform the Processor about any audits by and communication with supervisory authorities, insofar as this Agreement may be concerned. The Processor may pass this information on to the Sub-Processor. The Controller may only issue information to third parties including supervisory authorities upon prior consultation with the Processor.

7 Data protection officer, Representative

7.1 The Controller may be obliged to designate a data protection officer (hereinafter the DPO). Without particular request by the Processor the Controller shall inform the Processor about this DPO and any change of the DPO.

7.2 Where Article 3 (2) of the GDPR applies, the Controller may be obliged to designate in writing a representative in the European Union. Without particular request by the Processor the Controller shall inform the Processor about its representative and any change of the representative.

8 Persons acting under the authority of the Processor or Sub-Processor with access to Data

8.1 The Processor as well as the Sub-Processor on the Processor's behalf shall only deploy employees and other persons acting under the Processor's resp. Sub-Processor's authority for the processing of Data pursuant to this Agreement (hereinafter "personnel") who prior to the processing have committed themselves to

confidentiality and have been informed about legal provisions on data protection. The Processor and Sub-Processor shall ensure that any personnel process the Data according the provisions of this Agreement. Upon the Controller's request the Processor shall provide documentation hereof to the Controller or commission the Sub-Processor to do so.

8.2 Processor and Sub-Processor may process Data, in particular transfer Data if required to do so by EU law or Member State law to which the Processor or Sub-Processor is subject or if ordered by a court or state authority within the European Union.

9 General Principles regarding security of the processing

9.1 Upon the Controller's individual request, which the Processor may pass on to the Sub-Processor, the Processor, by means of the Sub-Processor, shall provide description of its technical and organizational measures to ensure security of processing (security concept of the Sub-Processor, **Attachment 2**) to the requesting Controller. In cases where the Sub-Processor commissions other sub-contractors pursuant to sec. 11, the Processor, by means of the Sub-Processor, shall request the other sub-contractors to provide their security concepts; upon request by the Controller the Processor, by means of the Sub-Processor, provides the sub-contractor's security concept to the requesting Controller.

9.2 The security concept shall meet at least the following requirements and provide detailed and specific provisions (see however section 9.3): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing for the Controller as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, appropriate technical and organisational measures, including inter alia as appropriate

a. the pseudonymisation and encryption of Data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to Data in a timely manner in the event of a physical or technical incident;
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing shall be implemented to ensure a level of security appropriate to the risk.

9.3 The Controller is able to enter or upload any categories of Data (e.g. attached files) without the Processor's or Sub-Processor's prior knowledge of the specific Data. The Controller is exclusively responsible to review such Data and assess their sensitivity and request a higher level of IT security.

9.4 The technical and organisational measures are subject to enhancements. They will be updated and adapted to the state of the technology, but must not drop below the level of security and protection outlined in this Agreement (in particular **Attachment 2**). Essential updates and adaptions will be documented.

9.5 If the Controller informs the Processor that this Agreement may also govern special categories of personal data, in particular data concerning health, the Processor will pass this information on to the Sub-Processor which shall review and assess the appropriate level of security and, if necessary, adapt the security measures and documentation in **Attachment 2**.

10 Controls

10.1 The Controller may request a qualified self-declaration (data protection report) of the Processor by an independent and unbiased entity (e.g. DPO, accountants/auditors, external data protection or quality auditors) in written or electronic format. As the Processor engages the Sub-Processor for the processing of the Controller's Data this data protection report contains the information necessary to determine this Sub-Processor's compliance with the obligations as set forth in Art. 28 GDPR, implementation and realization of the technical and organizational measures to ensure security of processing as set forth in **Attachment 2, in particular if special categories of personal data are concerned**.

10.1.1 The Controller is entitled to inspect the fulfilment of this Agreement, in particular the technical and organisational measures and documentations. Upon request by the Controller the Processor will immediately inform the Sub-Processor of this request. As the Processor does not have access to the Data that is object of this Agreement but the Sub-Processor has (see abovesec. 1.2), the Controller may inspect the Sub-Processor, by conducting on-site inspections during the Sub-Processor's regular business hours on Business Days at the Sub-Processor's premises. The Controller is entitled to involve an external auditor with contractual or statutory confidentiality obligations to conduct audits or parts of audits for the Controller.

10.1.2 The Controller shall carry out on-site inspections not more than once in three years and at more frequent intervals only if there are factual indications that the Processor or Sub-Processor violated the provisions set forth in this Agreement.

10.1.3 The Controller shall give notice to the Processor and Sub-Processor in written or electronic from at least seven (7) days prior and, if applicable, determining the factual indications the Controller deems given.

10.2 The Processor agrees to subject himself to controls of the supervisory authority of the Controller.

11 Sub-contractors

11.1 The Processor is hereby authorized to engage and commission the Sub-Processor. The Processor and the Sub-Processor concluded an agreement pursuant to Article 28 GDPR setting out essentially similar and appropriate data protection obligations as set out in this Agreement.

11.2 The Sub-Processor may also engage **another processor as sub-contractor**.

11.3 The Sub-Processor is authorized by the Processor to commission the sub-contractor **Deutsche Telekom GmbH (hereinafter "Telekom"), Landgrabenweg 151, 53227 Bonn**. The Sub-Processor and Telekom concluded a Data processing agreement substantially in the form of this Agreement setting out the same data protection obligations.

11.4 Where the Sub-Processor fails to fulfil its data protection obligations, the Processor shall 11.4 remain fully liable to the Controller for the performance of that sub-contractor's obligations.

12 Obligation to bear costs

The following support services resp. assistance to be provided by the Sub-Processor on behalf of the Processor for the Controller arising from individual instructions of the Controller are subject to appropriate fees and therefore require a prior explicit order of the Controller:

a. the support for the correction, deletion, restriction, transfer or return of Data due to sec. 5.2,
b. the support with the Data Protection Impact Assessment pursuant to sec. 5.4,
c. the support for the implementation of instructions due to sec. 5.2,
d. the assistance with the notification to the Supervisory Authority or data subjects pursuant to sec. 6.3,
e. the data protection reports as set forth in 10.1,
f. the support of legitimate on-site controls by the Controller or its auditor if the audit(s) reveal not more than unsubstantial non-conformance (in case the audit reveals substantial non-conformance the Processor shall bear proportionate costs);
g. the support for audits by supervisory authorities conducted either at the Sub-Processor or at the Controller pursuant section 10.2.

The Controller shall bear the costs for any such support services and assistance and shall reimburse the Processor.

13 Change Request

This Agreement and its Attachments may only be modified and amended in writing or electronically. The Processor shall be obliged to support and accept such modifications and amendments if they are required by law, in particular law applicable to the Processor.

14 Hierarchy

14.1 In case of contradictions or inconsistencies between this Agreement and the End User Agreement, this Agreement shall prevail and the following hierarchy shall apply:

1. Service-Specific Terms and Conditions
2. Service Specifications
3. this Agreement
4. other parts of the End User Agreement.

14.2 In case of contradictions or inconsistencies between this Agreement and its Attachments 1 to 2, this Agreement shall prevail and the following hierarchy shall apply:

1. this Agreement,
2. Attachment 1 and
3. Attachment 2.

15 Conclusion of this Agreement

With the Controller's acceptance by clicking the respective check box in the shopping cart this Agreement will be concluded between the Parties.

Attachment 1
Data subjects, types Of Data, extent of the processing

1. Categories of data subjects

1.1 Single or concurrent users of TestBench Cloud Service as a Service, in particular:

- Tester, Test Automation Engineers, Test Manager, Developer
- miscellaneous further persons working at a Controller's Tenant, e.g.: members of the accounting department, sales personnel

1.2 Other individuals whose personal data is entered or uploaded/attached by the Controller for the management, automation, design and execution of tests within test cases and test results or within the requirements of the system under test

- However, TestBench Cloud Service as a Service does not require that the Controller enters or uploads/attaches personal data insofar and the Processor recommends that the Controller only enters or uploads/attaches personal data for these purposes if necessary and limited to a minimum.

2. Types of Data

Types of Data are content Data of TestBench Cloud Service as a Service (see 2.1 - 2.5) and content Data of support requests or incident reports of the Controller (2.6) as

well as log files:

2.1 Data for User Management of TestBench Cloud Service as a Service:

- To identify and authorize the single current or concurrent users of the TestBench Cloud Service as a Service the Sub-Processor processes Name, Prename, User-ID, Password and E-Mail of single or concurrent users of the Controller

2.2 Data for Test planning and Test Management:

- With TestBench Cloud Service as a Service the Controller is able to plan who should design, automate or execute test cases and when and how this should happen

2.3 Data for Test design and Test Execution:

- As part of designing test cases the Controller is able to enter test case data. These test case data may be any kind of data. If needed by the Controller this may also include personal data and even special categories of personal data which the Controller is able to enter or upload (attachment of files). The Controller is solely responsible for the admissibility of processing (in particular entering and uploading) such personal data with TestBench Cloud Service as a Service.
- As part of executing test cases the Controller is able to enter or upload/attach any kind of data (such as screen shots, log files) describing the test results in more details including personal data or even special categories of personal data.
- The Controller is able to log personal data of the persons (single or concurrent users) who design or execute test cases with TestBench as a Cloud Service.

2.4 Requirements Management:

- As part of Requirements for the system under test (User Stories, EPICS, features) the Controller is able to enter or upload/attach personal data.
- The Controller is able to log personal data of the persons (single or concurrent users) who enter or upload requirements with TestBench Cloud Service as a Service.

2.5 Reporting-Functionality of TestBench Cloud Service as a Service:

- All data entered by the Controller into the TestBench Cloud Service as a Service may also be reported, both electronically and on paper. Those reports are

initiated by the Controller and provided to the Controller. Those reports may include any data entered by the Controller including personal data.

2.6 Maintenance Service and Support:

- Within support requests or reports of incidents the Controller transmits Name, Prename, User-ID, Password, E-Mail and – if applicable – a telephone number of the reporting/requesting single or concurrent user of the Controller.

3. Extent of the processing

3.1 Data processing on behalf of the Controller

- On behalf of the Controller and commissioned by the Processor, the Sub-Processor stores the content Data of TestBench Cloud Service as a Service (see 2.1 - 2.5) to be retrieved and displayed or reported to the Controller.
- The processing includes copies of this Data for backup and – if necessary – recovery purposes.
- Upon termination of the Controller's subscription and on request of the Controller, the Processor by means of the Sub-Processor provides the entered and uploaded/attached data in a machine readable and transferable format (on the Sub-Processor's choice either in XML or CSV format). After 4 weeks of termination of the Controller's subscription, the Sub-Processor will delete all data which belongs to the tenant and is stored in the operational data store. Depending on the agreed service level (number of backups to be maintained), the entire backup will be permanently deleted. Due to technical reasons, some data of the Controller stored in log files and transaction log entities cannot be deleted explicitly but will be deleted permanently as soon as the entire log file and transaction log entities are not needed any longer.

3.2 Analyse issues for support requests or in case of incident reports of the Controller:

- In the case of support requests or incident reports of Controllers or proactively if the Sub-Processor recognizes incidents or for regular maintenance services the Sub-Processor will access the relevant content Data of TestBench Cloud Service as a Service (see 2.1 - 2.5) and content Data of support requests or incident reports of the Controller (2.6) and relevant log files. The Sub-Processor will process this data for support or maintenance purposes.

3.3 Derive anonymized statistical KPIs:

- The Sub-Processor analyses and aggregates the entered user stories, test cases, test data, test results including defects of the system under test in an

anonymized way, to derive statistical data, which cannot be traced back neither to the end user nor to its tenant or an individual. Such anonymous statistical data are e.g. percentage of failed test cases per industry over time, or percentage of defects per user story per product category (e.g. mobile device app) over time .

Attachment 2

Technical and organisational security measures

1. The Controller is able to use TestBench Cloud Service as a Service via direct REST API calls or by using the provided web interface.
2. All requests of the Controller are processed by an application server (product: Akka), which is hosted at the Open Telekom Cloud and maintained by the Sub-Processor.
3. All communication between the Controller and the application server via the internet is secured by https.
4. The entered data is stored in a database (product: Cassandra) which is also hosted in the Open Telecom Cloud and maintained by the Sub-Processor.
5. Also backups, log files and any further data entered by the Controller into the TestBench Cloud Service as a Service are stored in the Open Telecom Cloud.
6. Even if extended system components which communicate with the application server are added in the future, this communication always will be secured by https and will use the secured inbound network of the Open Telekom Cloud.
7. Even if extended system components which communicate with the systems of the Controller are added in the future, this communication always will be secured by https and the outbound communication will be secured by firewalls or similar systems.
8. The Processor by means of the Sub-Processor provides a more detailed description of its technical and organisational security measures until May 24, 2018 or earlier upon a Controller's explicit request.