Data Processing Agreement

Agreement on the processing of personal data on behalf of a controller pursuant to Art. 28 GDPR

Preamble

This Data Processing Agreement and its Annexes (“DPA”) reflects the agreement with respect to the Processing of Personal Data in the sense of the General Data Protection Regulation (" GDPR") by the contractor JonnyGit GmbH, Lohmühlenstraße 65, 12345 Berlin (also referred to as "we", "us", "service", “data processor”, "JonnyGit”) on behalf of Customer (also referred to as "client", “data controller”). The Contractor shall provide services to the Customer in accordance with the Agreement concluded between them (hereinafter also referred “Main Contract") and in accordance with the General Terms and Conditions. In order to meet the requirements of the GDPR for such constellations, the parties shall conclude the following Data Processing Agreement, which shall become effective upon signing the Agreement.

The Customer and the JonnyGit hereinafter each also referred to as "Party" and jointly as "Parties".

We periodically update these terms. If you have an active JonnyGit subscription, we will let you know when we do via email (if you have subscribed to receive email notifications) or via in-app notification. You can find archived versions of the terms here.

§ 1 Subject/scope of the agreement

(1) Within the scope of the cooperation between the parties in accordance with the main contract, the contractor has access to personal data of the client (hereinafter "client Data"). The Contractor shall process this client data on behalf of and in accordance with the instructions of the client within the meaning of Art. 4 No. 8 and Art. 28 GDPR.

(2) The processing of the client data by the contractor is carried out in the following manner and to the extent and purpose specified therein. The group of persons affected by the data processing is limited to the groups of persons involved in software development at the customer and is represented accordingly. The duration of the processing corresponds to the duration of the main contract.

a. Purpose of the processing

- Process mining of process data in Git repositories in the context of software development processes. This includes in particular the documentation and analytical processing of process data.
- User management for access control and contacting
- Support in the execution of agreements or orders

b. Categories of data subjects

- Employees including former employees as well as trainees and interns
- External service providers and consultants and freelancers

c. Categories of personal data

- Process data (meta-data with information about actions and interactions of individual developers in the software development process, such as log data), especially authors and timestamps and file names on created or modified files, as well as information about specific changes to these files).
- Names and user identifications

- Organizational information about departmental affiliations
- E-mail addresses

(3) The Contractor is prohibited from processing client data deviating from the above-mentioned specifications.

(4) The processing of the client data takes place exclusively within the territory of the Federal Republic of Germany, in a member state of the European Union or in another state party to the Agreement on the European Economic Area. Should there be a relocation of the order processing to a third country, this requires the prior consent of the client and only takes place if the special requirements of Art. 44 to 49 GDPR are fulfilled. The client already agrees to the processing of personal data by the subcontractors listed below upon conclusion of this contract.

(5) The provisions of this contract apply to all activities related to the main contract. The same shall apply to all activities in which the Contractor and its employees or agents commissioned by the Contractor come into contact with Client data.

§ 2 Authority of the client

(1) The contractor processes the client data within the scope of the order and on behalf of and according to the instructions of the client in the sense of Art. 28 GDPR (order processing). The client has the sole right to issue instructions on the type, scope and method of the processing activities (hereinafter also referred to as "right to issue instructions"). If the contractor is obliged by the law of the European Union or the member states to which he is subject to further processing, he shall notify the customer of these legal requirements prior to processing.

(2) Instructions are generally given by the client in writing or in electronic form (e-mail is sufficient); instructions given orally must be confirmed by the contractor in electronic form.

(3) If the contractor is of the opinion that an instruction of the client violates data protection regulations, he must inform the client of this fact. The contractor is entitled to suspend the execution of the instruction in question until it is confirmed or amended by the client.

§ 3 Protective measures of the contractor

(1) The contractor is obliged to comply with the legal provisions on data privacy and not to pass on information obtained from the customer's area to third parties or to suspend their access. Documents and data must be secured against unauthorized access, taking into account the state of technology.

(2) Furthermore, the Contractor shall oblige all persons entrusted by it with the processing and performance of this contract (hereinafter referred to as "employees") to maintain confidentiality (obligation of confidentiality, Art. 28 para. 3 lit. b GDPR). At the request of the client, the contractor shall provide the client with written or electronic evidence of the obligation of the employees.

(3) The Contractor shall design its internal organisation in such a way that it meets the special requirements of data privacy. He undertakes to take all appropriate technical and organisational measures for the appropriate protection of the client data in accordance with Art. 32 GDPR, in particular the measures listed in Annex 1 to this contract, and to maintain these measures for the duration of the processing of the client data.

(4) The contractor reserves the right to change the technical and organisational measures taken, whereby he shall ensure that the contractually agreed level of protection is not compromised.

(5) At the request of the client, the contractor will provide the client with evidence of compliance with the technical and organisational measures.

§ 4 Information and support obligations of the contractor

(1) In the event of disruptions, suspicion of data protection violations or breaches of contractual obligations on the part of the Contractor, suspicion of security-related incidents or other irregularities in the processing of the Client's data by the Contractor, persons employed by the Contractor within the framework of the order or by third parties, the Contractor shall inform the Client immediately, but at the latest within 48 hours, in writing or electronically. The same applies to audits of the Contractor by the data protection supervisory authority. These notifications should in each case contain at least the information referred to in Art. 33 para. 3 GDPR.

(2) In the above-mentioned case, the Contractor shall support the Client in the performance of its educational, remedial and information measures in this respect within the scope of what is reasonable.

(3) The Contractor undertakes to provide the Client, at its request and within a reasonable period of time, with all information and evidence required to carry out an audit.

§ 5 Other obligations of the contractor

(1) If the conditions of Art. 30 GDPR apply to the contractor, the contractor is obliged to keep a record of all categories of processing activities carried out on behalf of the customer in accordance with Art. 30 Para. 2 GDPR. The list shall be made available to the customer on request.

(2) The Contractor is obliged to assist the Client in the preparation of a data privacy impact assessment pursuant to Art. 35 GDPR and any prior consultation of the supervisory authority pursuant to Art. 36 GDPR.

(3) The contractor confirms that he has appointed a data protection officer - insofar as there is a legal obligation to do so. The Customer must be informed of any change in the person of the company data protection officer/contact person for data protection.

(4) Should the Customer's data at the Contractor be endangered by seizure or confiscation, by insolvency or settlement proceedings or by other events or measures of third parties, the Contractor must inform the Customer immediately, unless this is prohibited by court or official order. In this context, the Contractor shall inform all responsible authorities without delay that the decision-making authority over the data lies exclusively with the Customer as the "responsible party" within the meaning of the GDPR.

§ 6 Sub-Processors

(1) The Contractor is authorised to establish subcontracting relationships with subcontractors ("subcontracting relationship") within the scope of its contractual obligations. The Contractor shall ensure that the provisions agreed in this contract also apply to the subcontractors engaged by him, whereby the Client shall be granted all rights of control over the subcontractor in accordance with this contract.

(2) A subcontractor relationship within the meaning of these provisions shall not exist if the contractor commissions third parties with services which are to be regarded as purely ancillary services. These include, for example, postal, transport and dispatch services, cleaning services, security services, telecommunications services without any specific reference to services which the contractor provides for the customer as well as other measures to ensure the confidentiality, availability, integrity and resilience

of the hardware and software of data processing systems. The Contractor's obligation to ensure compliance with data protection and data security also in these cases remains unaffected.

(3) The contractor has established subcontractor relationships with the following companies, which the client agrees to by concluding this data processing agreement:

- Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg

§ 7 Rights of inspection

(1) The client is entitled to regularly ensure that the regulations of this contract are complied with. For this purpose, he may, for example, request information from the Contractor, have existing attestations from experts, certifications or internal tests presented to him or have the Contractor's technical and organizational measures checked personally or by a competent third party during normal business hours, provided that the latter is not in a competitive relationship with the Contractor.

(2) The client will only carry out checks to the extent necessary and will take appropriate account of the contractor's operating procedures. The parties shall agree on the time and type of inspection in good time.

(3) The client shall document the results of the inspection and notify the contractor. In the event of errors or irregularities which the client discovers, particularly in the examination of the results of the order, he must inform the contractor without delay. If facts are discovered during the inspection, the future avoidance of which requires changes to the ordered procedure, the client shall inform the contractor immediately of the necessary procedural changes.

§ 8 Rights of data subjects

(1) The Contractor shall support the Client as far as possible with suitable technical and organisational measures in the fulfilment of the Client's obligations under Articles 12 to 22 and Articles 32 to 36 GDPR. He shall provide the Client with the requested information on Client data without delay, but at the latest within 14 working days, unless the Client himself has the relevant information at his disposal.

(2) If the person concerned asserts his rights in accordance with Art. 16 to 18 GDPR, the Contractor is obliged to rectify, delete or restrict the Client's data without delay, at the latest within a period of 7 working days, on the Client's instructions. The Contractor shall provide the Client with written proof of the deletion, correction or restriction of the data upon request.

(3) If a data subject asserts rights, such as the right to information, rectification or deletion with regard to his data, directly against the contractor, the contractor shall forward this request to the client and await the client's instructions. In the absence of such specific instructions, the Contractor shall not contact the data subject.

§ 9 Term and termination

The term of this contract corresponds to the term of the main contract. If the main contract can be terminated with notice, the provisions for ordinary termination shall apply accordingly.

§ 10 Deletion and return after termination of contract

(1) The Contractor shall return to the Customer after termination of the main contract or at any time at the Customer's request all documents, data and data carriers provided to him or, at the Customer's

request, delete them completely and irrevocably, unless a statutory retention period exists. This also applies to copies of the Customer's data at the Contractor's premises, such as data backups, but not to documentation that serves as proof of the orderly and proper processing of the Customer's data. Such documentation shall be kept by the Contractor for a period of 6 months and shall be handed over to the Client upon request.

(2) The Contractor shall confirm the deletion to the Client electronically. The purchaser has the right to control the complete and contractually compliant return or deletion of the data at the contractor in a suitable manner.

(3) The Contractor is obliged to treat confidentially the data which have become known to him in connection with the main contract also beyond the end of the main contract.

§ 11 Liability

(1) The liability of the parties is governed by Art. 82 GDPR. Any liability of the Contractor towards the Client due to breach of obligations arising from this contract or the main contract remains unaffected.

(2) The parties shall each release themselves from liability if one party proves that it is in no way responsible in any way for the circumstance by which the damage occurred to a party affected. This shall apply accordingly in the case of a fine imposed on one party, whereby the release shall be to the extent that the respective other party bears part of the responsibility for the infringement sanctioned by the fine.

§ 12 Final provisions

(1) The parties agree that the defence of the right of retention by the contractor in the sense of § 273 German Civil Code (BGB) with regard to the data to be processed and the associated data carriers is excluded.

(2) Changes and amendments to this agreement must be made in electronic form.

(3) In case of doubt, the provisions of this agreement shall take precedence over the provisions of the main contract. Should individual provisions of this agreement prove to be wholly or partially invalid or unenforceable, or become invalid or unenforceable as a result of changes in legislation after conclusion of the contract, the validity of the remaining provisions shall not be affected. The invalid or unenforceable provision shall be replaced by a valid and enforceable provision which comes as close as possible to the meaning and purpose of the invalid provision.

(4) This agreement is subject to German law. Exclusive place of jurisdiction is the registered office of the contractor.

Annexes

Annex 1 - Technical and organisational measures of the Contractor (Art. 32 GDPR)

In addition to the order processing contract, the parties shall make the following specifications regarding the technical and organisational measures to be implemented by JonnyGit:

Confidentiality (Art. 32 para. 1 lit. b GDPR)

Entry control

The following measures prevent unauthorized persons from gaining access to data processing systems:

- Access control system, badge reader (magnetic/chip card)
- Door safety devices (electric door openers, combination lock, etc.)
- Key management/documentation of key allocation
- Alarm system
- Special protection measures of the server room (Certification according to ISO/IEC 27001:2013, 27017:2015, 27018:2019 and ISO/IEC 9001:2015)
- Special protective measures for the storage of backups and other data carriers
- Non-reversible destruction of data media

Access control

The following measures prevent unauthorised third parties from having access to data processing systems:

- Personal and individual authentication when logging on to the system/network
- Authorization process for acces rights
- Password procedure (specification of password parameters regarding complexity and update interval)
- Logging of the access
- Additional login for certain applications (especially administrator rights and server administration)
- Automatic blocking of clients after time lapse without user activity
- Hardware firewall
- Use of a state-of-the-art software firewall
- Use of state-of-the-art anti-virus software
- Mobile Device Policy

Authorization control

The following measures ensure that unauthorized third parties do not have access to data:

- Conclusion of contracts for order processing for the external care, maintenance and repair of data processing systems, provided that in the case of remote maintenance the processing of data is the subject of the service provided by the contractor.
- Evaluations/Logging of data processing
- Authorization process for permissions
- Encryption of data carriers
- Dual control principle
- Segregation of Duties
- Number of people with administrator status minimized
- Privacy shields for mobile data processing systems
- Blocking of accounts of former employees

Separation control

The following ensure that data collected for different purposes are processed separately:

- Multi-tenancy of IT systems
- Use of test data
- Separation of development and production environment

Integrity (Art. 32 para. 1 lit. b GDPR)

Transfer control

It is ensured that data cannot be read, copied, changed, removed or otherwise processed without authorisation during transmission or storage on data carriers and that it is possible to check which persons or bodies have gained access to data. The following measures have been implemented to ensure this:

- Encryption of e-mail or e-mail attachments
- Encryption of data media
- Secured file transfer or other data transport
- Encrypted WLAN
- Logging of data transmission or data transport
- Logging of read accesses
- Logging the copying, modification or removal of data

Input control

The following measures ensure that it can be verified who has processed data in data processing systems at what time:

- User access rights
- System side logging

Availability and resilience (Art. 32 para. 1 lit. b GDPR)

The following measures ensure that data is protected against accidental destruction or loss and is always available to the customer:

- Security concept for software and IT applications
- Backup procedure
- Redundant data storage
- Guarantee of data storage in the secured network
- Apply security updates as needed
- Uninterruptible Power Supply (UPS)
- Fire and/or fire water protection of the server room
- Air-conditioned server room
- Virus protection
- Firewall
- Resilience of the systems is guaranteed by oversizing

Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

Data Privacy Management

The following measures are intended to ensure that there is an organisation that meets the basic requirements of data privacy law:

- Obligation of employees to maintain confidentiality
- Adequate training of employees in data protection
- Keeping a register of processing activities (Art. 30 GDPR)
- Privacy mission statement of JonnyGit
- Privacy Guideline of JonnyGit

Data Breach Management

The following measures should ensure that reporting processes are triggered in the event of data protection violations:

- Notification process for data breaches pursuant to Art. 4 No. 12 GDPR to the supervisory authorities (Art. 33 GDPR)
- Notification process for data protection infringements pursuant to Art. 4 No. 12 GDPR with regard to data subjects (Art. 34 GDPR)

Privacy-friendly default settings (Art. 25 para. 2 GDPR)

Privacy-conscious presettings must be taken into account both in the standardized presettings of systems and apps and in the setup of processing. In this phase, functions and rights are specifically configured, the permissibility or inadmissibility of certain entries or possible entries is determined with regard to data minimization, and a decision is made on the availability of usage functions. In the same way, the type and scope of the reference to persons or anonymization (e.g. in the case of selection, export and evaluation functions, which are defined and preset or freely configurable) or the availability of certain processing, functions or logs are determined.

Order control

The following measures ensure that data is only processed according to the instructions of the customer:

- Agreement on data processing with regulations on the rights and obligations of the parties
- Process for issuing and/or following instructions
- Determination of contact persons and/or responsible employees
- Training/instruction of all employees with access rights at JonnyGit
- Obligation of employees to maintain confidentiality
- Agreement of contractual penalties for breaches of instructions

As of: July 27, 2020