www.orderbird.com
hello@orderbird.com

Data Processing Agreement

between

_____

_____

(name)

_____

(address)

-Principal-

and

orderbird AG

Ritterstraße 12-14. Aufg. 4

10969 Berlin

-Contractor-

Preamble

By contract of _____ (hereinafter referred to as “Main Contract”), the Parties, inter alia, established an obligation regarding data processing. By present Processing Agreement, the obligations of the Parties regarding data protection are to be stipulated in detail.

The Parties agree that this Agreement will apply to all activities arising in connection with the processing of personal data under the Main Contract and which are performed by employees or agents of the Contractor.

1. Subject matter of the Agreement

(1) The Contractor shall process personal data on behalf of the Principal. This shall include the data collected in the course of use of the Contractor’s software which are in the Principal’s possession.

(2) Any remuneration is conclusively stipulated in the underlying Main Contract.

(3) In essence, the assignment of the Principal refers to the data processing period of data “storage” which are processed in various procedures.

(4) Customer and employee data (e.g. name, company name, customer number, address) as well as, where applicable, communication data (e.g. e-mail address, telephone number) and contract billing and payment data will be processed as personal data.

(5) The relevant categories of persons of the data subjects include customers and employees of the Principal.

2. Provision of data by the Principal

The Principal will provide the data via the orderbird.POS client application and the “my.orderbird” administration and accounting tool. It shall ensure that the access data for the data base are stored safely and not disclosed to third parties. Access is only possible to the contractual data. After termination of the Contract, the Contractor shall destroy the access data.

3. Rights and obligations of the Principal

(1) In the course of this Contract, the Principal shall be solely responsible for assessment of reliability of data processing as well as for the protection of data subjects’ rights.

(2) For this purpose, the Principal and Contractor shall agree upon the technical and organisational measures enclosed to this Agreement as attachment. The Principal shall ensure that such measures provide a level of security appropriate to the risks to the data processed; in particular, it shall ensure that the confidentiality, integrity, availability and resilience of the systems and services are permanently ensured in connection with the processing.

(3) The Principal shall be entitled to issue instructions on the type, scope and methods of data processing in written or electronic form. The instructions shall by stipulated by the Agreement upon commencement of cooperation. In the course of the assignment, the Principal may issue individual instructions on the protection of personal data and check compliance with the data protection regulations and the instructions stipulated by it. Oral instructions shall be confirmed in writing or in text form without any delay.

(4) The Principal shall designate to the Contractor a person authorised to issue instructions.

(5) The Principal shall inform the Contractor without undue delay if it determines errors or irregularities during examination of the order results.

(6) The Principal shall be obliged to keep confidential any knowledge of business secrets and data security measures of the Contractor obtained in the course of the contractual relationship.

4. Obligations of the Contractor

(1) The Contractor shall process personal data only in accordance with the agreements made and subject to the Principal's instructions, unless provided otherwise by legal provisions.

(2) The Contractor shall inform the Principal without undue delay if it is of the opinion that an instruction is in breach of legal provisions. The Contractor may suspend implementation of an instruction until it is confirmed or changed by the Principal.

(3) The Contractor will not use the data provided for data processing for any other purposes than those set forth above. No copies or duplicates will be created without the Principal's knowledge.

(4) The Contractor shall design its internal business organisation such that it meets the statutory requirements regarding data protection.

(5) In its scope of responsibility, the Contractor shall ensure implementation of and compliance with the general and technical and organisational measures for the protection of the Principal's data agreed upon and attached to this Agreement, taking into account the legal requirements. This shall also include the use of a method for regular checking, assessing and evaluating the efficiency of the technical and organisational measures in order to ensure security of the processing in line with legal requirements.

(6) The Contractor shall be entitled to unilaterally change the security measures taken; in the course thereof, it has to be ensured that at least the level of protection contractually agreed upon is in place.

(7) The Contractor shall, at the Principal's request, support the Principal in the fulfilment of data protection obligations to the extent legal provisions stipulate such support by the Contractor.

(8) The Contractor shall ensure that employees and other persons acting on the Contractor's behalf responsible for processing data of the Principal are not allowed to process the data contrary to instructions. Furthermore, employees and the third parties acting on behalf of the Contractor shall be obliged to secrecy, unless they are subject to a comparable legal obligation of secrecy. These provisions shall continue in force after completion of the assignment.

(9) The Contractor shall inform the Principal without undue delay about technical and organisational insufficiencies of data protection and in case of any suspicion of data protection breaches or other irregularities regarding the processing of the personal data. It shall take the required measures to protect the data and to mitigate adverse consequences for the data subjects and shall immediately coordinate with the Principal for the purpose thereof.

(10) The Contractor shall rectify, erase or block personal data if this is requested by the Principal in an instruction. If erasure or restriction of data processing in line with data protection legislation is not possible, the Contractor shall be responsible for destruction of the

data carriers and other materials affected in line with data protection legislation subject to an individual assignment from the Principal or shall return such data carriers to the Principal. In specific cases to be determined by the Principal, such data carriers shall be stored; then, the remuneration and protective measures shall be agreed upon separately.

(11) After completion of the assignment, the Contractor shall hand over to the Principal any results of processing or use connected to the assignment relationship which come into its possession. Thereafter, the Principal's data carriers shall be physically destroyed. Testing and reject materials shall be destroyed or handed over to the Principal without undue delay. The erasure and/or destruction shall be confirmed to the Principal in writing, stating the date. Legal retention obligations shall remain unaffected by this Agreement.

5. Verification possibilities

(1) The Principal shall be entitled, after coordination with the Contractor, to perform checks itself or have an auditor engaged by it perform tests and to verify the Contractor's compliance with this Agreement in its business operation by spot checks which are to be announced in a timely manner.

(2) The Contractor shall prove to the Principal compliance with the obligations stipulated in this Agreement by performing self-audits. It shall store such audits for the Principal and transfer them to a contact person designated by the Principal upon request.

6. Subcontractors

(1) The use of subcontractors for the fulfilment of the contractual obligations of the Contractor shall be permissible and subject to prior notification of the Principal.

(2) The Contractor shall enter into agreements with such third parties to the required extent in order to ensure appropriate data protection and information security measures.

(3) To the extent the subcontractor renders its services outside the EU / EEA, the Contractor shall ensure permissibility thereof under data protection legislation by appropriate measures.

7. Information obligations

If the protection of personal data is endangered by measures of third parties, e.g. by insolvency proceedings or other events, the Contractor shall notify the Principal without undue delay. The Principal's property (e.g. data carriers, working copies, containers) shall be marked in a timely manner.

8. Contractual term

The term of this Agreement shall commence upon contract conclusion and shall end upon termination of the Main Contract entered into between the Parties.

9. Liability and damages

Liability provisions agreed upon between the Parties in the Main Contract shall also apply to this Processing Agreement, unless specifically agreed upon otherwise.

www.orderbird.com
hello@orderbird.com

10. Termination

In the event of severe or repeated breaches of this Agreement, the Parties shall be entitled to a reciprocal right of extraordinary termination.

11. Written-form clause, choice of law

(1) Changes and amendments to this Agreement and all components thereof shall be in writing; this may also be in electronic form.

(2) In case of any contradictions, provisions in this Data Protection Annex shall take precedence over the provisions in the Main Contract.

(3) If individual parts of this Annex are invalid, this shall not affect the validity of the remainder of the Annex.

(place and date)	(place and date)
	Berlin 22.11.18
for the Principal	for orderbird AG

www.orderbird.com
hello@orderbird.com

Technical and

Organisational Measures

Organisations which process, use or collect personal data themselves or on behalf of another party shall implement the technical and organisational measures which allow for processing operations in line with data protection legislation. Measures shall only be required if appropriateness is ensured upon balancing of the protection interests.

orderbird AG meets such requirement by the following measures; we differ between our own measures and the measures in the data centres used by us which are operated by processors.

Version: 2 August 2018

www.orderbird.com
hello@orderbird.com

I. Our own measures

We take the following measures to the extent the processing activities are not performed by processors:

1. Confidentiality, integrity, availability (Art. 32(2) point (b) GDPR)

a) Entry control

No.	Technical Measures	Organisational Measures
1.	Chip-card/transponder system	Written and unambiguous key management with clear responsibility of employees known by name
2.	Safe storage of keys/key safe	Regular examination of entry authorisations granted
3.	Safety locks	Reception/visitors are accompanied by employees
4.		Selection and monitoring of watch and cleaning services in terms of data protection aspects

b) Admission control

No.	Technical Measures	Organisational Measures
1.	Encryption of notebooks/laptops	Password policy incl. increased requirements to length, complexity and change
2.	Authentication with personalised access data	
3.	Automatic blocking	

	in case of unsuccessful login attempts	
5.	Use of firewalls for the protection of IT systems	
6.	Use of VPN for remote accesses to IT systems	
7.	Data deletion system for deletion by disk utilities (Mac OS) or DBAN (Server)	
8.	Logging of accesses to applications and IT systems	
9.	Ensuring hard disk encryption	
10.	Enforcing screensaver login	
11.	Option of remote deletion by mobile-device management (MDM)	
12.	Distribution of firmware passwords (EFI passwords)	

c) Access control

No.	Technical Measures	Organisational Measures
1.	Logging of accesses to applications and IT systems	Grouping of the access authorisations by area of functions or responsibilities
2.	Logging of failed attempts at accessing IT systems	Authorisation concept for accesses to IT systems
3.	Regulated and technically reliable destruction of data by using a “data bin”	Password policy and protected password assignment

4.		Administration of user rights by trained system administrators
5.		Assignment of rights by trained personnel
6.		Regular review of access authorisations for IT systems
7.		Authorisation concept with minimum principle

d) Separation control

No.	Technical Measures	Organisational Measures
1.	Permanent assignment of processing devices to individual applicants	Different workplaces for different processing operations and categories of data
2.	Systems with multi-client capability for separation of functions	Control via authorisation concept
3.	Segmentation of networks by need for protection	Customer contractual data will be stored in separate CMS with their own access authorisation system
4.	Separation of developing and testing environments and production systems	Test data will be generated in the development in order not to have to resort to live data
5.		Determination of database rights

e) Disclosure control

No.	Technical Measures	Organisational Measures
1.	E-mail encryption for sensitive data (e.g. for communication with payroll office)	Documentation of the data recipients as well as of the duration of planned provision and of the erasure periods

2.	Use of VPN	Disclosure in appropriate cases in pseudonymised or anonymised form
3.	Provision of information via encrypted connections such as https, sftp	
4.	Use of signature processes	

2. Availability and reliability control (Art. 32 (c) GDPR)

No.	Technical Measures	Organisational Measures
1.	Use of systems provided on a redundant basis	Retention of data backups at a secure, outsourced location
2.	Fire extinguishers in offices and infrastructure rooms in place	Monitoring of all relevant infrastructure and IT systems
3.	Use of data mirroring (RAID) for relevant IT systems	Backup and recovery concept (formulated)
4.		Control of the backup process
5.		Regular tests for data restoration and logging of the results

3. Incident response management

No.	Technical Measures	Organisational Measures
1.	Use of firewalls and regular updating thereof	Documented process for the identification and reporting of security incidents/data breaches (also with regards to the notification obligation towards the supervisory authority), “Incident Response Policy”
2.	Use of VPN	Documented procedure for handling

		of security incidents
3.	Provision of information via encrypted connections such as https, sftp	Involvement of the data protection officer in security incidents and data breaches, process of continuous improvements
4.	Use of signature processes	Formal process for subsequent reviews of security incidents
5.		Documentation of security incidents in the ticket system

4. Order control (outsourcing to third parties)

No.	Technical Measures	Organisational Measures
1.	E-mail encryption for sensitive data	Examination of the security measures taken by the contractor the documentation thereof
2.	Use of VPN	Formal process for the examination and conclusion of processing agreements or EU standard contractual clauses
3.	provision of information via encrypted connections such as https, sftp	Written instructions to contractors
4.	Use of signature processes	Obligation of the contractor's employees to data secrecy shall be ensured
5.		Contractual guarantee of destruction of data upon assignment completion
6.		Process for ongoing monitoring of processors

5. Data protection management (Art. 32 (d) GDPR)

No.	Technical Measures	Organisational Measures
1.	Documentation of the processes electronically retrievable	Regular awareness-raising of the employees regarding data protection issues
2.	Technical logging of entry, changes and erasure of data	Established data destruction/data erasure process
3.	Manual and automated control for logging files created for this purpose in software	Regular examination of policies for currency and effectiveness
4.	Central documentation of the processes and work instructions relevant to data protection; access possibility for the employees in question, depending on relevance	Established dismantling process for product terminations
5.	Ensuring the data minimisation principle on the technical level; in request processes, only the required data are required to be entered by employees	Onboarding and offboarding policies for new and departing employees
6.		Centralised monitoring of compliance with the adequate level of data protection at processors
7.		External consulting by specialist law firm
8.		“Mobile Work” policy, binding under labour law, with special precautions against data loss and unauthorised access by third parties

9.		Use policy regarding means of work/data carriers
10.		External data protection officer
11.		Retention of forms from which data were integrated into automated processing operations
12		Employees trained and obliged to confidentiality/data secrecy

II. Measures by our processors

For the performance of our core business, we use the services of industry-leading cloud providers. At the point of time of conclusion of this Agreement, these are the following companies, US companies being self-certified under the Privacy Shield Agreement:

Amazon Web Services, Inc. 410 Terry Ave North Seattle, WA 98109-5210	Cloudflare, Inc. 101 Townsend St. San Francisco, CA 94107

Our subcontractors engaged in the course of data processing take the following technical and organisational measures. Where there are no uniform measures, this is emphasised by an abbreviation to indicate the subcontractor in question (A = Amazon Web Services Inc., C = Cloudflare Inc.):

1. Confidentiality, integrity, availability (Art. 32(2) point (b) GDPR)

   a) Entry control

No.	Technical Measures	Organisational Measures
1.	Entry control system	Control of persons entering the company premises and the data centres[A]

2.	Two-stage authentication with personalised access data[A]	Allocation system for admission cards for employees and persons with special authorisation
3.	Locking system with security locks	At least two-stage authentication before admitting access to data centres required[A]
4.	Video surveillance of the entrances and exits[A], intrusion detection system	Allocation of entry rights for employees and externa employees based upon defined criteria
5.		Allocation and documentation of the authorisations via access rights management
6.		Identity registration for visitors and external employees[A]
7.		Accompanying of visitors and external employees only by authorised employees[A]
8.		Documentation and auditing of any accesses occurred[A]

b) Admission control

No.	Technical Measures	Organisational Measures
1.	Use of firewalls for the protection of IT systems	Authorisation concept for admission to data processing systems, allocation of authorisations subject to defined criteria
2.	Use of VPN for remote accesses to IT systems	Password policy and protected password allocation
3.	Logging of accesses to servers,	Automated temporary blocking of the user

	networks, ports	terminals if not used, identification and password entry required for repeated opening[C]
4.	Use of encryption processes	Automated temporary blocking of the user authorisation in case of repeated input of incorrect passwords, logging of password entries[C]
5.	Remote access to internal IT system only after authentication, use of VPN'A	
6.		Alerting of competent employees in case of suspicious accesses[A] Use of pagers for alerting[A] Uninterrupted availability of competent employees[A] weekly discussions on the implementation of preventive measures[A]
7.		Disposal of disused data carriers in accordance with defined requirements[A]

c) Access control

No.	Technical Measures	Organisational Measures
1.	Logging of accesses to applications and IT systems	Concept for access authorisations by area of functions and responsibilities
2.	Logging of suspicious attempts at accessing information-processing systems, notification to competent employees[A]	Provision of an Incident Management Team[A]
3.	Optional: access only possible after multi-factor authentication[A]	Employee policies and individual trainings regarding access rights[C]

4.	FIPS 140-2-compliant SSL load balancers[A]	Possibility of logging persons who erasure, add or modify personal data[C]
5.	Implementation of network devices for administrating interface communication with internet service providers (ISPs)[A]	
6.	Redundant connection to several communication services of the network[A]	
7.	Use of encryption technologies (Security Socket Layers (SSL)[A])	

d) Separation control

No.	Technical Measures	Organisational Measures
1.	Separation of operative and corporate network[A], Separate data storage on data base level by module, customer or supported function[C]	Allocation of access authorisations for different networks via ticketing system[A] and authorisation concept
2.	Access to operational network only with SSH public key authentication[A]	automated cessation of the authorisation after 90 days or upon resignation of the employee from the company[A]
3.	Restriction of interfaces, batch processes and reports for certain purposes and functions[C]	

e) Disclosure control

No.	Technical Measures	Organisational Measures
1.	Access protection for systems on operational and	Release of data only to authorised

	corporate level[A]	persons, including allocation of differentiated access rights and roles[C]
2.	Use of firewalls, VPN and encryption technologies for the protection of the gateways and pipelines via which the data are transferred	Controlled and documented erasure of the data[C]
3.	Encryption of certain employee data (e.g. personally identifiable information such as national ID numbers, credit or debit card numbers) within the network[C]	Notification of the user in case of incomplete data transmission (end-to-end check)[C]
4.		Logging of data transmission (if possible)[C]

2. Availability and reliability control (Art. 32 (c) GDPR)

No.	Technical Measures	Organisational Measures
1.	Interruption-free and redundant electricity supply for the data centres without impacts on ongoing processes[A], System for uninterruptable power supply (UPS) in case of an electric breakdown for critical and substantial loads in the system-A, Generators for the data centres can supply electricity to the entire system[A]	Monitoring and regular maintenance of the electrical, mechanical and vital systems and devices for immediate error identification[A]
2.	Redundant network infrastructure[C]	Separate backup security[C]
3.	Automated fire detection system with smoke detectors and extinguishing equipment in	Monitoring of temperature and humidity in the data centre by employees[A]

	date centre environments, mechanical and electrical infrastructure rooms, cooling rooms and generator equipment rooms[A], Protection by wet pipe, double-locking or gas sprinkler systems[A]	
4.	Air conditioning of the data centres[A]	Cluster distribution of the data centres worldwide[A] Exclusion of “cold” data centres, all are active[A]
5.	System for monitoring the temperature and humidity in data centres[A]	Automated system for relocating the customer data traffic from the affected area in case of disruptions[A]
6.	N+1 configuration ensuring that there is sufficient capacity to relocate the data traffic to the remaining sites in case of shutdown of a data centre[A]	Provision of several geographical availability zones for data backup, feeding of the zones via different networks of independent utility companies[A]
7.	Redundant connection of the availability zones with several tier-1 transit providers[A]	Geographical separation of availability zones in typical metropolitan areas and establishment of availability zones in flood areas with low risk[A]
8.	Maintenance of systems for generating backups in the data centres[A]	Possibility of data storage in different availability zones[A]
9.		Regular examination of the availability and reliability of the systems within the group[A]

10.		Performance of security audits and penetration tests[A]
11.		Routine, emergency and configuration changes to the existing infrastructure will be authorised, logged, tested, approved and documented in accordance with industry standards for similar systems[A]
12.		Requirements regarding the customer information in case of required changes[A]

3. Incident response management

No.	Technical Measures	Organisational Measures
1.	Use of firewalls and regular updating thereof[A]	Incident Management Team[A]
2.	Use of VPN[A]	Use of industry-standard diagnosis processes[A]
3.	Provision of information via encrypted connections[A]	Availability of the Incident Management Team around the clock[A]
4.	Use of signature processes (optional)[A]	Formal process for subsequent reviews of security incidents[A]
5.		Documentation of security incidents in the ticket system[A]
6.		Incident Response Policy[A]

4. Input control

No.	Technical Measures	Organisational Measures

1.		Authorisation policy for entering, reading, changing and erasing data[C]
2.		Input authorisation management[C]
3.		Password policy[C]
4.		Authentication requirement of the authorised personnel[C]
5.		Protective measures for data input in the storage as well as for reading, changing and erasing stored data[C]
6.		Logging of entries made[C]

5. Data protection management (Art. 32 (d) GDPR)

No.	Technical Measures	Organisational Measures
1.	Documentation of the processes electronically retrievable[A]	
2.	Technical logging of the entry, change and erasure of data[A]	
3.	Manual and automated control of logging files created for this purpose in softwares[A]	