Annex 1

Exhibit on technical and organisational security measures in accordance with Article 32 of the GDPR

Data is processed exclusively on the servers in the data centers at the various locations. The measures in the areas of access control may therefore differ depending on the location, but compliance with the required level of protection is guaranteed in any case.

The measures according access control and transfer control apply to data traffic between the data centers, customer access to the systems and system administration by Byteplant employees.

1. Access control (persons)

Measures to ensure that unauthorised persons do not gain access to the data processing equipment used to process personal data:

#	Recommended measures	Measure implemented	Annotations
1	Determination of authorized access groups, authorization concept	X	by data center operator
2	Protection even outside working hours (e.g. alarm system)	X	by data center operator
3	Access protection (e.g. alarm system)	X	by data center operator
4	Protection of access routes and door protection (e. g. electric door closer, card reader, television monitor, gatekeeper)	X	by data center operator
5	Measures to secure the building (e.g. safety glazing, alarm system, site security, patrol services)	X	by data center operator

2. Access Control (IT system)

Measures to ensure that unauthorised persons are prevented from using the data processing equipment and procedures refer to intrusion into the IT system itself:

#	Recommended measures	Measure implemented	Annotations
1	Determination of differentiated access regulations (e. g. for employees, external parties)	X	by data center operator
2	Lockability of data processing systems (e. g. server room)	X	by data center operator
3	Securing the network against external access (e.g. firewalls), Intrusion Prevention System, Einrichtung einer demilitarisierten Zone)	X	
4	Securing screen workstations (e.g. screen locking)	X	
5	Functional and/or time-limited use of systems and identification features (end of a session after a specified inactive time; after multiple incorrect password entries)	X	
6	Regulation for user authorization	X	
7	Encryption of networks (e. g. VPN; password-protected WLANs)	X	

#	Recommended measures	Measure implemented	Annotations
8	Encryption of remote maintenance and access	X	

3. Access control (authorized accesses)

Measures to ensure that those authorised to use the data processing procedures can only access the personal data subject to their right of access and that the data used during processing cannot be read, copied, changed or removed without authorisation:

#	Recommended measures	Measure implemented	Annotations
1	Determination of data access rights by means of an authorization concept	X	Only administrators have access rights.
2	Identification of authorised accesses to the data processing system (e. g. passwords, access codes)	X	
3	Definition of the authorization for data entry, modification, deletion (depending on the role assignment: reading, writing, deleting)	X	
4	General agreement or service instructions for handling passwords, mobile devices, private e-mails; screen locks	X	Regulated by agreement or service instruction to all employees: rules for handling passwords no use of mobile devices Obligation to use screen locks no use of business email accounts for private purposes.

4. Transfer control

Measures to ensure that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or during transport or storage on data media and that it can be verified at which points the transmission of personal data by means of data transmission facilities is envisaged:

#	Recommended measures	Measure implemented	Annotations
1	Encryption of data and connections (e. g. encrypted connection via the Internet)	X	
2	B Authorization concept (definition of authorized persons for data transfer)	X	
3	Control by employees (principle of dual control)	X	
4	Definition of the areas in which data carriers must or may be located		no external data carriers are used
5	Securing the areas in which data carriers are located, for example, during transport/transfer		no external data carriers are used
6	Identification of the persons who may remove data carriers from these areas		no external data carriers are used.
7	Differentiated management of data carriers, inventory control		no external data carriers are used.
8	Documentation on the points to which a transmission is envisaged, the transfer channels and transfers of data	X	
9	Customer communication by email takes place exclusively via office desktops. Mobile / private devices are not permitted.		Regulated by instructions to all employees.
10	Deletion of data remainders before data medium exchange	X	overwrite

5. Entering control

Measures to ensure that it is possible to verify and establish at a later stage whether and by whom personal data have been entered, modified or removed in data processing systems.

#	Recommended measures	Measure implemented	Annotations
1	Identification of recorded data (e. g. date and user ID, content)		The data is entered exclusively by the client.
2	Organizational definition of responsibilities for entering data		The data is entered exclusively by the client.
3	Control of access rights	X	
4	Regulations on retention periods for audit and other verification purposes		No data is stored permanently; Data is deleted and overwritten after processing.

6. Order / Assignment control

Measures to ensure that personal data processed on behalf of the customer can only be processed in accordance with the instructions of the customer:

#	Recommended measures	Measure implemented	Annotations
1	Written contract between client and contractor	X	
2	Regulation of the rights and obligations of the contractor and client	X	
3	Process for issuing and/or following instructions	X	

7. Availability control

Measures to ensure that personal data is protected against accidental destruction or loss:

#	Recommended measures	Measure implemented	Annotations
1	definition of responsibilities	X	
2	Inform employees about emergency plans and conduct tests and exercises	X	by data center operator
3	Data Backup/Backup Concepts		Customer data is excluded from backup for data protection reasons.
4	Regular testing of emergency generators and surge protection	X	by data center operator
5	Monitoring the operating parameters of data centers	X	by data center operator

8. Separation requirement

Measures to ensure that personal data collected for different purposes can be processed separately. There is no need for physical separation. A logical separation is sufficient.

#	Recommended measures	Measure implemented	Annotations
1	Separation of client data on IT systems	X	1) at data center level: by data center operator 2) at system level: Batch: Order ID Online API: API key
2	Functional separations	X	
3	Separation of development, test and production system	X	
4	Programming regulations	X	
5	Regulations for system and program testing	X	

9. Evaluation (art. 32. (1) lit., art. 25 (1) GDPR)

Procedures for the regular review, evaluation and evaluation of the effectiveness of technical and organisational measures:

#	Recommended measures	Measure implemented	Annotations
1	Data Protection Management	X	
2	Auditing by the data protection officer	X	annually and, if necessary, additionally in the event of major changes
3	Regular training of employees	X	

10. Other measures

#	Recommended measures	Measure implemented	Annotations
1	Presence of concepts, guidelines and work instructions (e. g. data protection concept)	X	
2	Commitment of employees to confidentiality	X	
3	Maintain a record of processing activities (art. 30 GDPR)	X	
4	Carry out an assessment of the impact of the envisaged processing operations (art. 35 GDPR)	X	
5	Process for Notification of a personal data breach to the supervisory authority	X	