Data Processing Agreement

Contract for commissioned processing pursuant to Art. DSGVO

Instructions for completing: Print out the contract or save the document as a PDF.

Have it signed by the relevant person and send it as a PDF with the subject „DPA" to support@vinitycard.com

Status: Februar 2024

Standard Contractual Clauses SECTION I

Clause 1

Purpose and scope of application

a) These standard contractual clauses ("Clauses") are intended to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, on the free movement of such data and repealing Directive 95/46/EC (the "General Data Protection Regulation").

b) The controllers and processors listed in Annex I have agreed to these clauses to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

c) These clauses apply to the processing of personal data in accordance with Annex II.

d) Annexes I to IV form an integral part of the Clauses.

e) These clauses are without prejudice to the obligations to which the controller is subject under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

f) These clauses do not in themselves ensure compliance with the obligations relating to international data transfers under Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2 Unalterability of the clauses

a) The parties undertake not to amend the clauses except to supplement or update the information given in the annexes.

b) This does not prevent the parties from incorporating the standard contractual clauses set out in these clauses into a more comprehensive contract and from adding further clauses or additional guarantees, provided that these do not directly or indirectly conflict with the clauses or interfere with the fundamental rights or freedoms of the data subjects.

Clause 3 Interpretation

a) Where terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 are used in those clauses, those terms shall have the same meaning as in that Regulation.

b) These clauses are to be interpreted in the light of the provisions of Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 respectively.

c) Those clauses shall not be interpreted in a way that is contrary to the rights and obligations provided for in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 or that affects the fundamental rights or freedoms of data subjects.

Clause 4 Precedence

In the event of any conflict between these clauses and the provisions of any related agreements existing between the parties or subsequently entered into or concluded, these clauses shall prevail.

SECTION II OBLIGATIONS OF THE PARTIES

Clause 5

Description of the processing

The details of the processing operations, in particular the categories of personal data and the purposes for which the personal data are processed on behalf of the controller, are set out in Annex II.

Clause 6

Obligations of the parties

6.1. Instructions

a) The processor shall process personal data only on the documented instructions of the controller, unless it is required to process under Union law or the law of a Member State to which it is subject. In such a case, the processor shall notify the controller of those legal requirements prior to the processing, unless the law in question prohibits it on grounds of important public interest. The controller may give further instructions throughout the processing of personal data. These instructions shall always be documented.

b) The processor shall inform the controller without undue delay if it considers that instructions given by the controller infringe Regulation (EU) 2016/679, Regulation (EU) 2018/1725 or applicable Union or Member State data protection law.

6.2. Earmarking

The Processor shall process the Personal Data only for the specific purpose(s) set out in Annex II, unless it receives further instructions from the Controller.

6.3. Duration of the processing of personal data

The data shall be processed by the processor only for the duration specified in Annex II. The duration of this contract (term) corresponds to the term of the performance agreement.

6.4. Processing safety

a) The processor shall implement at least the technical and organisational measures set out in Annex III to ensure the security of personal data. This includes the protection of the data against a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of or access to the data, whether accidental or unlawful (hereinafter a personal data breach). In assessing the appropriate level of protection, the Parties shall have due regard to the state of the art, the costs of implementation, the nature, scope, circumstances and purposes of the processing, and the risks involved for the data subjects.

b) The Processor shall only grant its Personnel access to the Personal Data subject to the Processing to the extent strictly necessary for the performance, management and monitoring of the Contract. The Processor shall ensure that the persons authorised to process the Personal Data received have committed themselves to confidentiality or are subject to an appropriate legal duty of confidentiality.

6.5. Sensitive data

Where the processing concerns personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, or containing genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning a person's health, sex life or sexual orientation, or data concerning criminal convictions and offences (hereinafter "sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

6.6. Documentation and compliance with clauses

a) The parties must be able to demonstrate compliance with these clauses.

b) The Processor shall deal promptly and reasonably with requests from the Controller relating to the processing of Data under these Clauses.

c) The Processor shall provide the Controller with all information necessary to demonstrate compliance with the obligations set out in these Clauses and arising directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the request of the controller, the processor shall also allow and contribute to the audit of the processing activities covered by these clauses at reasonable intervals or where there are indications of non-compliance. When deciding on a review or audit, the controller may take into account relevant certifications of the processor.

d) The controller may conduct the audit itself or engage an independent auditor. Audits may include inspections of the Processor's premises or physical facilities and shall be carried out, where appropriate, with reasonable advance notice.

e) The Parties shall make the information referred to in this clause, including the results of audits, available to the relevant supervisory authority or authorities upon request.

6.7. Use of subcontracted processors

a) The Processor shall not subcontract any of its processing operations carried out on behalf of the Controller pursuant to these Clauses to a sub-processor without the prior separate written authorisation of the Controller. The Processor shall submit the request for the separate authorisation at least one month before the sub-processor in question is engaged, together with the information required by the Controller to decide on the authorisation. The list of sub-processors approved by the Controller is set out in Annex IV and the Parties shall keep Annex IV up to date.

b) Where the Processor engages a sub-processor to carry out certain processing activities (on behalf of the Controller), such engagement shall be by way of a contract which imposes substantially the same data protection obligations on the sub-processor as those applicable to the Processor under these Clauses. The Processor shall ensure that the Sub-processor complies with the obligations to which the Processor is subject under these Clauses and under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The Processor shall provide the Controller with a copy of any such subcontracting agreement and any subsequent amendments upon the Controller's request. To the extent necessary to protect trade secrets or other confidential information, including personal data, the Processor may obscure the wording of the agreement before providing a copy.

d) The Processor shall be fully liable to the Controller for the Sub-processor's compliance with its obligations under the contract concluded with the Processor. The Processor shall notify the Controller if the Sub-processor fails to perform its obligations under the Contract.

e) The Processor shall agree with the Sub-processor on a third party beneficiary clause, according to which the Controller - in the event that the Processor ceases to exist factually or legally or is insolvent - has the right to terminate the subcontract and instruct the Sub-processor to delete or return the personal data.

6.8. International data transfers

a) Any transfer of data by the processor to a third country or an international organisation shall only be made on the basis of documented instructions from the controller or to comply with a specific provision under Union law or the law of a Member State to which the processor is subject and shall comply with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

b) The Controller agrees that where the Processor uses a sub-processor pursuant to clause 6.7 for the performance of certain processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor may ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission pursuant to Article 46(2) of Regulation (EU) 2016/679, provided that the conditions for the application of those standard contractual clauses are met.

Clause 7

Support of the responsible person

a) The processor shall immediately inform the controller of any request received from the data subject. He shall not respond to the request himself unless he has been authorised to do so by the controller.

b) Taking into account the nature of the processing, the processor shall assist the controller in fulfilling the controller's obligation to respond to requests from data subjects to exercise their rights. In fulfilling its obligations under points (a) and (b), the processor shall follow the instructions of the controller.

c) In addition to the Processor's obligation to assist the Controller under Clause 7(b), the Processor shall, taking into account the nature of the Data Processing and the information available to it, also assist the Controller in complying with the following obligations:

1. Obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (hereinafter "data protection impact assessment") where a form of processing is

likely to result in a high risk to the rights and freedoms of natural persons;
2. Obligation to consult the competent supervisory authority(ies) prior to processing where a data protection impact assessment indicates that the processing would result in a high risk, unless the controller takes measures to mitigate the risk;
3. Obligation to ensure that personal data is accurate and up to date by the processor informing the controller without delay if it becomes aware that the personal data it processes is inaccurate or out of date;
4. obligations under Article 32 of Regulation (EU) 2016/679.

d) The Parties shall set out in Annex III the appropriate technical and organisational measures for the Processor's assistance to the Controller in the application of this Clause and the scope and extent of the assistance required.

Clause 8

Notification of personal data breaches

In the event of a personal data breach, the Processor shall cooperate with and provide appropriate assistance to the Controller to enable the Controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or, where applicable, Articles 34 and 35 of Regulation (EU) 2018/1725 , taking into account the nature of the processing and the information available to the Processor.

8.1. Violation of the protection of data processed by the controller

In the event of a personal data breach in relation to the data processed by the Controller, the Processor shall assist the Controller as follows:

a) in notifying the personal data breach to the competent supervisory authority or authorities without undue delay after the controller becomes aware of the breach, where relevant (unless the personal data breach is unlikely to result in a risk to the personal rights and freedoms of individuals);

b) in obtaining the following information to be included in the notification by the responsible person pursuant to Article 33(3) of Regulation (EU) 2016/679, which information shall include at least the following:

1)the nature of the personal data, where possible, with an indication of the categories and approximate number of data subjects and the categories and approximate number of personal data sets concerned;

2)the likely consequences of the personal data breach;

3)the measures taken or proposed by the controller to address the personal data breach and, where appropriate, measures to mitigate its possible adverse effects.

If and to the extent that all such information cannot be provided at the same time, the initial notification shall contain the information available at that time and further information shall be provided thereafter without undue delay as and when it becomes available;

c) in complying with the obligation under Article 34 of Regulation (EU) 2016/679 to notify the data subject without undue delay of the personal data breach where that breach is likely to result in a high risk to the rights and freedoms of natural persons.

8.2. Violation of the protection of data processed by the processor

In the event of a personal data breach in relation to the data processed by the Processor, the Processor shall notify the Controller without undue delay after becoming aware of the breach. This notification shall contain at least the following information:

a) a description of the nature of the breach (specifying, if possible, the categories and the approximate number of individuals concerned and the approximate number of data sets concerned);

b) Contact details of a contact point where further information about the personal data breach can be obtained;

c) the likely consequences and the measures taken or proposed to remedy the personal data breach, including measures to mitigate its possible adverse effects.

If and to the extent that all such information cannot be provided at the same time, the initial notification shall contain the information available at that time and further information shall be provided thereafter without unreasonable delay as and when it becomes available.

The Parties shall set out in Annex III any other information to be provided by the Processor to assist the Controller in fulfilling its obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III

FINAL PROVISIONS

Clause 9

Breaches of the clauses and termination of the contract

a) Without prejudice to the provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, if the Processor fails to comply with its obligations under these clauses, the Controller may instruct the Processor to suspend the processing of personal data until it complies with these clauses or the contract is terminated. The processor shall immediately inform the controller if, for whatever reason, it is unable to comply with those clauses.

b) The Controller shall be entitled to terminate the Contract insofar as it concerns the processing of personal data pursuant to these Clauses if

1. the controller has suspended the processor's processing of personal data pursuant to point (a) and compliance with those clauses has not been restored within a reasonable period of time and in any event within one month of the suspension;
2. the Processor materially or persistently breaches these Clauses or fails to comply with its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
3. the Processor fails to comply with a binding decision of a competent court or the competent supervisory authority(ies) concerning its obligations under these Clauses, Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The Processor shall be entitled to terminate the Contract insofar as it concerns the processing of Personal Data pursuant to these Clauses if the Controller insists on the performance of its instructions after having been notified by the Processor that its instructions are in breach of applicable legal requirements pursuant to Clause 6.1(b).

d) Upon termination of the contract, the Processor shall, at the choice of the Controller, erase all personal data processed on behalf of the Controller and certify to the Controller that this has been done, or return all personal data to the Controller and erase existing copies, unless there is an obligation under Union or Member State law to retain the personal data. Until the deletion or return of the data, the processor shall continue to ensure compliance with these clauses.

ANNEX I

List of parties

Responsible person(s): [name and contact details of the responsible person(s) and, if applicable, the data protection officer of the responsible person].

Company: _____

Firstname: _____

Lastname: _____

E-Mail: _____

Position: _____

Processor:

vinitycard

Address: Attilastraße 177, 12105 Berlin

Name, function and contact details of contact person: Colaker, Burak & Colaker, Mert GbR, e-mail: info@vinitycard.com

ANNEX II

Description of the processing

Categories of data subjects whose personal data are processed: Employees

Categories of personal data processed:

· First name and surname

· Address (official)

· Telephone number (business)

· Mobile phone number (business)

· E-mail address (official)

· Function

· Photo(s)

· User names of the personal social media channels

· Other personal data stored in the profile by the person responsible or his/her employees.

Sensitive data processed (if applicable) and restrictions or safeguards applied that take full account of the nature of the data and the risks involved, e.g. strict purpose limitation, access restrictions (including access only for staff who have undergone specific training), records of access to the data,

Restrictions on onward transfers or additional security measures n/a

Type of processing

· Use of the personal data to create a digital web-based business card, storage of the personal data in a data centre, transmission of the data contained in the business card to desired recipients via individual internet link, in the email signature, via vCard or via QR code in the vinitycard app Purpose(s) for which the personal data are processed on behalf of the controller

· Provision of a digital, web-based business card (website)

Duration of the processing Term of the contract

ANNEX III

Technical and organisational measures, including to ensure the security of data

Description of the technical and organisational security measures (including any relevant certification) implemented by the controller(s) to ensure an adequate level of protection, taking into account the nature, scope, context and purposes of the processing and the risks to the rights and freedoms of natural persons:

· Measures to ensure non-public database access

· Measures to ensure database access only for authorised staff and only by means of 2-factor authentication

· Measures to ensure the security of processing

· Measures to protect data during storage

· Measures of encrypted transmission of personal data

· Measures to protect data during transmission

· Measures of pseudonymisation, in the collection and processing of information for the improvement of the application

· Measures for the random generation of user IDs

· Measures for the random generation of product IDs

· Measures of encrypted storage of user passwords

· Measures to mitigate brute force attacks on user accounts

· Measures for the identification and authorisation of users

· Measures to ensure the continued confidentiality, integrity, availability and resilience of systems and services in relation to processing

· Measures to ensure the ability to rapidly restore the availability of and access to the personal data in the event of a physical or technical incident, except in the case of deletion by the controller

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

· Measures to ensure the physical security of places where personal data are processed

· Measures to ensure the logging of events

· Measures to ensure system configuration, including default configuration

· Measures for the internal governance and management of IT and IT security

· Measures to ensure data minimisation

· Measures to ensure data quality

· Measures to ensure limited data retention

· Measures to ensure accountability

· Measures to enable data portability and to ensure erasure

See also "Checklist of technical and organisational measures" in Annex V.

In the case of data transfers to (sub)processors, the specific technical and organisational measures to be taken by the (sub)processor to support the controller shall also be described.

Description of the specific technical and organisational measures to be taken by the processor to support the controller:

· Measures to ensure the security of processing

· Measures to protect data during storage

· Measures for the identification and authorisation of users

· Measures to ensure the continued confidentiality, integrity, availability and resilience of systems and services in relation to processing

· Measures to ensure the ability to rapidly restore the availability of and access to the personal data in the event of a physical or technical incident, except in the case of deletion by the principal

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

· Measures to ensure the physical security of places where personal data are processed

· Measures to ensure the logging of events

· Measures to enable data portability and to ensure erasure

· Measures to ensure data quality

· Measures to ensure accountability

See also "Checklist of technical and organisational measures" in Annex V.

Annex V: Technical and organisational measures (checklist)

A. Measures to ensure confidentiality and integrity 1.

Access control measures to server rooms 1.0

Is personal data of the principal stored on servers operated by you or any service providers?

? yes ? no

If no: In this case, the further questions on A1 do not have to be answered, but the questions from A2 onwards must be answered immediately. The questions on B1 and B2 are also omitted.

1.1

Location of the server room / data centre (RZ). Frankfurt and Nuremberg

1.2

Is the personal data distributed across more than one server location / data centre (e.g. backup server / use of cloud services)?

? yes ? no

1.3

If yes: Please provide the corresponding location information also regarding further servers. Further server locations:

1.4

Does the following information on access control measures apply to all server / data centre locations in use?

? yes ? no

1.5

Is the server room alarm-protected by means of an intruder alarm system (EMA)?

? yes ? no

1.6

If yes: Who is informed when the EMA triggers? Multiple answers possible!

? commissioned security guard ? administrator ? head of IT ? other:

1.7

Is the server room under video surveillance?

? yes, without image recording ? yes, with image recording ? no 1.8

Is the server room equipped with an electronic locking system?

? yes ? no, with mechanical lock

1.9

If yes: Which access technology is used? Multiple answers possible!

? RFID ? PIN ? Biometrics ? Other:

1.10

If yes: Are access rights assigned on a personalised basis?

? yes ? no

1.11

If yes: Are accesses to the room logged in the access system?

? yes, both successful and unsuccessful access attempts

? yes, but only successful entries

? yes, but only unsuccessful access attempts

? no, the lock is only released or not

1.12

Is the server room used for other purposes besides its actual function?

? yes ? no

1.13

If yes: What else is stored in the server room?

? Telephone system ? Storage of office supplies ? Storage of files ? Archive

? Storage of IT equipment ? Other:

1.

Access control measures to office premises 2.1

Location of client workstations from which personal data is accessed: Access exclusively via VPN

2.2

Is there a porter service / permanently manned reception area to the building or to your offices?

? yes ? no

2.3

Is a visitors' book kept?

? yes ? no

2.4

Is the building or the offices alarmed by means of a burglar alarm system (EMA)?

? yes ? no

2.5

If yes: Who is informed when the EMA triggers?

? commissioned security guard ? administrator ? head of IT ? other:

2.6

Is the office building or its entrances under video surveillance?

? yes, without image recording ? yes, with image recording ? no

2.7

If "yes, with image recording", how long is the image data stored?

3

Access and access control measures 3.1

Is there a process for assigning user IDs and access authorisations when new employees are hired and when employees leave or in the event of organisational changes?

? defined release process

? No defined approval process, on demand

? Other methods of award:

3.2

Are the allocation or changes of access authorisations logged?

? yes ? no

3.3

Do employees authenticate themselves to the central directory service via an individual identifier?

? yes ? no

3.4

Do binding password parameters exist in the company?

? yes ? no

3.5

Password character length: 50

Does the password have to contain special characters?

? yes ? no

Minimum validity period in days: 90

3.6

Does the IT system force the user to comply with the above PW requirements? x yes ? no

3.7

Is the screen locked when the user is inactive? If so, after how many minutes?

10 minutes

3.8

What measures do you take if a password is lost, forgotten or spied out?

? Admin assigns new initial password

? none

3.9

Is there a limit on unsuccessful login attempts?

? yes, 3 attempts ? no

3.10

If so, how long will accesses remain blocked once the maximum number of unsuccessful login attempts has been reached?

? The accesses remain blocked until the block is manually lifted

? The entrances remain locked for please enter value in minutes minutes.

3.11

How is authentication carried out for remote access: Authentication with ? Token ? VPN certificate ? Password

3.12

Is there a limit on unsuccessful login attempts for remote access?

? yes, 3 attempts?no 3.13

If so, how long will accesses remain blocked once the maximum number of unsuccessful login attempts has been reached?

? The accesses remain blocked until the block is manually lifted

? The accesses remain locked for please enter value in minutes minutes.

3.14

Is remote access automatically disconnected after a certain period of inactivity?

? yes, after 30 minutes? no

3.15

Are the systems on which personal data are processed secured via a firewall?

? yes ? no

3.16

If yes: Is the firewall regularly updated?

? yes ? no

3.17

If yes: Who administers your firewall?

? Own IT ? External service provider

4

Measures to secure paper documents, mobile data carriers and mobile terminals 4.1

How are paper documents with personal data that are no longer needed (e.g. printouts / files / correspondence) disposed of?

? Waste paper / Residual waste

? Shredders are available for this purpose and their use is instructed.

? Locked data bins are set up, which are collected by a disposal service provider for destruction in compliance with data protection regulations.

? Other:

4.2

How are data carriers (USB sticks, hard drives) that are no longer needed and on which personal data are stored disposed of?

? Physical destruction by own IT.

? Physical destruction by external service provider.

? Deleting the data

? Delete data by please specify number of overwrites

? Other:

4.3

May mobile data carriers be used in the company (e.g. USB sticks)?

? yes

? no

4.4

Are employees allowed to use private data carriers (e.g. USB sticks)?

? generally yes

? yes, but only after approval and verification of the storage medium by IT.

? no, all required storage media are provided by the company.

4.5

Is personal data encrypted on mobile devices?

? Encryption of the hard disk

? Encryption of individual directories

? No measures 4.6

Do employees also process personal data on their own private devices (bring your own device)?

?

yes ? no

5

Measures for secure data transmission 5.1

Is the transfer of personal data consistently encrypted?

? not at all

? no, data transmission is via MPLS

? Only isolated

? by encrypted file as mail attachment

? via PGP / S/MIME

? via encrypted data carrier

? via VPN

? via https/TLS

? via SFTP

? Other:

5.2

Who manages the keys or the certificates?

? Users themselves? Own IT? External service provider

5.3

Are the transmission processes logged?

?

yes ? no

5.4

If 5.3 yes: How long is this log data kept? please enter value in days Days

5.5

If 5.3 yes: Are the logs evaluated regularly?

? yes ? no, but an evaluation would be possible if necessary

B. Measures to ensure availability 1.

Server room 1.1

Does the server room have a fireproof or fire-retardant access door? yes ? no

1.2

Is the server room equipped with smoke detectors? yes ? no

1.3

Is the server room connected to a fire alarm centre? yes ? no

1.4

Is the server room air-conditioned? yes ? no

1.5

Does the server room have an uninterruptible power supply (UPS)? yes ? no

2

Backup and emergency concept, virus protection 2.1

Does a backup concept exist?

? yes ? no

2.2

Is the functionality of the backup restore regularly tested?

? yes no

2.3

At what frequency are backups made of the systems on which personal data are stored?

? Real-time mirroring ? daily ? one to three times a week

? Other:

2.4

What kind of backup media are the backups stored on?

? Second redundant server ? Backup tapes ? Hard disks

? Other:

2.5

Where are the backups stored?

? Second redundant server is at a different location ? Safe, fireproof, data carrier and document secure

? simple safe ? safe deposit box ? locked filing cabinet / desk

? In the server room ? Private household ? Other:

2.6

Re 2.5: In case of a transport of the backups: How is this carried out?

? Take home by an employee of IT / management / secretary

? Collection by third parties (e.g. bank employees / security companies)

? Other: There is no physical transport

2.7

Are the backups encrypted?

? yes ? no

2.8

Is the location of the backups in a separate fire compartment or part of the building from the primary server?

? yes ? no

2.9

Is there a documented process for software or patch management?

? yes? no? Process exists, but is not documented

2.10

If 2.9 yes, who is responsible for software or patch management?

? Users themselves? Own IT? External service provider

2.11

Is there an emergency concept (e.g. emergency measures in case of hardware defects / fire / total loss etc.)?

? yes ? no

2.12

Are the IT systems technically protected against data loss / unauthorised data access? Yes, by means of constantly updated ? virus protection ? anti-spyware ? spam filters

2.13

If 2.12 yes, who is responsible for the current virus protection, anti-spyware and spam filter?

? Users themselves? Own IT? External service provider

3

Grid connection 3.1

Does the company have a redundant internet connection?

? yes ? no

3.2

Are the individual locations of the company redundantly connected with each other?

? yes ? no

3.3

Who is responsible for the company's grid connection?

? Own IT? External service provider

C. Pseudonymisation/encryption, Art. 32 para. 1 lit. a DSGVO 1.

Use of pseudonymisation 1.1

Are processed personal data pseudonymised?

? yes ? no

If 1.1 no: In this case, the other questions on C1 do not have to be answered, but the questions from C2 onwards must be answered immediately.

1.2

Are algorithms used for pseudonymisation?

? yes ? no 1.3

If 1.1 yes: Which algorithm is used for pseudonymisation?

1.4

Is there a separation of allocation data and storage in separate systems?

? yes ? no

1.5

How can pseudonymisation be reversed if necessary? Multiple answers possible!

? according to a defined procedure

? in the multi-eye principle

? Direct access to non-pseudonymised raw data

? On the instructions of the superior

? Other:

1.

Use of encryption 2.1

Is personal data processed encrypted beyond the measures already described?

? yes passwords ? no

If 2.1 is no: In this case, the other questions on C2 do not have to be answered, but the questions from D1 onwards must be answered immediately.

2.2

What types of encryption are used? Multiple answers possible! In case of multiple answers, please describe in the field "Other" which type of encryption is used for which data.

? End-to-end encryption ? Transport encryption ? Data-at-rest encryption

? Other: please enter.

2.3

Which cryptographic algorithms are used for encryption or encryption-like measures (e.g. hashing of passwords)?

? AES ? SHA-256 ? RSA-2048 or higher ? Other:

2.4

Who has access to the encrypted data?

Employees from the departments: please enter. A total of 0 employees have access to the encrypted data

D. Other measures according to Art. 32 (1) lit. b, c, d DSGVO 1.

Resilience

Measures are in place to ensure the ability to ensure the resilience of the systems and services related to the processing on an ongoing basis.

? no

? yes Monitoring, regular load tests, IP blocking

2

Recoverability

Are there contingency or recovery plans and measures in place beyond B.2.11 to ensure the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident?

? no

? yes , daily backups

3

Procedures for review, assessment and evaluation of the measures taken 3.1

Is there a procedure in place to regularly review, assess and evaluate the effectiveness of the technical and organisational measures to ensure the security of the processing?

? no

? yes

3.2

If 3.1 yes: At what intervals do the reviews take place? In case of changes to the infrastructure, otherwise every 6 months

3.3

If 3.1 yes: Are the results of the tests documented?

? yes ? no

3.4

Are there certifications with reference to the technical-organisational measures and if so, which ones?

? yes

? no

ANNEX VI

List of sub-processors

The controller has authorised the use of the following sub-processors:

Name: XXXXX

Address: XXXX GmbH, XXXXSTR. XX, XXXXX XXXX, Germany

Name and contact details of contact person: XXXXX, e-mail: XXXX [mailto:data-XXXXX]

Processing Description: Hosting, Computing, Storage, DBaaS, Kubernetes

Name: XX

Address: XXX XXXX GmbH, XXXXSTR. XX, XXXX XXXX, Germany Name and contact details of contact person: Elisabetta Castiglioni, email: info@vinitycard.com Description of processing: Hosting, Computing, Storage, DBaaS, Kubernetes

Name: XXXXX

Address: XXXX, XXXXXXXXXXXXXXXX Name and contact details of contact person:

XXXX XXXXXX, Data Protection Officer, e-mail: XXXXXXXX Description of processing: Mailing

Name: XXXXXXX

Address: XXXXXXXXXXXXXXX Name and contact details of contact person:

XXXXXXX, Data Protection Officer, e-mail: XXXXXXX Description of processing: CRM, Mailing, Ticket System

Name: XXX

Address: XXXXXXXXX, Germany

Name and contact details of contact person: XXXXXXXXXX Description of processing: Process Automation, DBaaS, Storage

ANNEX VII

List of sub-processors in case of special (non-standard) configurations

The following subcontractors are not active in the standard. Only if your company or organisation has explicitly ordered or activated an integration, API or otherwise this service with us, they are part of your GCU.

In the case of the use of "XXXX":

Name: XXXXXX

Address: XXX Attn: Legal Department/Privacy, XXXXXXXXXXXX Contact Name and Contact Information:

XXXXXXXXX, Data Protection Officer, e-mail: XXXXX [mailto XXXXXX]

In the case of the use of "Google Ads" or "Google Analytics": Name: Google Ireland Limited

Address: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland Name and contact details of contact person:

Nicholas Leeder, Managing Director, e-mail: support-deutschland@google.com

In case of using "SAP Integration" Name: HE-S Digital Management GmbH

Address: Marienstraße 7, 63867 Johannesberg, Germany Name and contact details of contact person:

Rinaldo Heck, Managing Director, e-mail: support@he-s.com

In case of use of "Personio" Name: Personio GmbH & Co. KG

Address: Personio GmbH & Co. KG, Rundfunkplatz 4, 80335 Munich, Germany

Name and contact details of the contact person:

Hanno Renner, Managing Director, e-mail: support@presonio.com