Data Processing Agreement (“DPA“)
Door James

[CGI Legal Entity Name]
Leinfelder Straße 60, 70771 Leinfelden-Echterdingen
Tel: +49 711 72846-0 | Fax: +49 711 72846-846

cgi.com/de

Data Processing Agreement (“DPA“) between

The Controller:

CGI Deutschland B.V. & Co. KG
[address]

- hereinafter referred to as the „**Client**“ -

and

The Processor:

CGI Deutschland B.V. & Co. KG
Leinfelder Straße 60, 70771 Leinfelden-Echterdingen

- hereinafter referred to as the „**Supplier**“ -

Sitz der Gesellschaft: Leinfelden-Echterdingen | Handelsregister: AG Stuttgart HRA 732235 | St.-Nr.: 97109/60377 | USt-ID: DE 114 118 368
Persönlich haftende Gesellschafterin: CGI General Partner B.V./ Niederlande, Rotterdam KvK 74017632

Content

§1 DEFINITIONS, SUBJECT MATTER AND DURATION

(1) Definitions

Unless otherwise defined herein, any words in capitalized letters herein shall have the meaning defined in the GDPR or in other applicable laws.

“**CGI Group**” means CGI Inc (1350 René-Lévesque Blvd West, 15th floor, Montréal, H3G 1T, Canada) and its affiliates engaged in the Processing of Personal Data hereunder.

“GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

For the purposes of this DPA, “GDPR” shall be construed as also referring to the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (“UK GDPR”) (in this DPA, any references to specific articles of the GDPR shall be construed as also referring to the equivalent sections of the UK GDPR, where applicable).

“**Processor Binding Corporate Rules**” or “**P-BCR**” mean the binding corporate rules of CGI formally approved July 22, 2021, by the French Supervisory Authority (CNIL) based on the Opinions of the European Data Protection Board (EDPB) published under https://www.cgi.com/de/de/datenschutz/binding-corporate-rules.

“**Standard Contractual Clauses**” or “**SCC**” mean Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

(2) Subject matter

The Subject matter of this DPA results from the Klicken oder tippen Sie hier, um Text einzugeben. which is referred to here (hereinafter referred to as “Main Contract”).

(3) Duration

The duration of this DPA corresponds to the duration of the Main Contract.

§2 SPECIFICATION OF DPA DETAILS

(1) Nature and Purpose of the intended Processing of Data

Nature and Purpose of Processing of personal data by the Supplier for the Client are precisely defined in the Main Contract and the ANNEX 1 hereto.

The undertaking of the contractually agreed Processing of Data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every Transfer of Data to a Country which is not a Member State of either the EU or the EEA requires the prior agreement of the Client and shall only occur if the specific conditions of Article 44 et seq. GDPR have been fulfilled. Such countries (if any) and the applicable appropriate safeguards of Article 44 et seq. GDPR regarding the adequate level of protection in those countries are named in ANNEX 2 and/or ANNEX 4.

(2) Type of Data

The type of personal data used is precisely defined in the Main Contract and the ANNEX 1 hereto.

(3) Categories of Data Subjects

The Categories of Data Subjects are precisely defined in the Main Contract and the ANNEX 1 hereto.

§3 TECHNICAL AND ORGANIZATIONAL MEASURES

(1) Before the commencement of processing, the Supplier shall document the execution of the necessary Technical and Organizational Measures, set out in advance of the awarding of this DPA, specifically with regard to the detailed execution of the DPA, and shall present these documented measures to the Client for inspection. Upon acceptance of this DPA by the Client, the documented measures become the foundation of the DPA. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.

(2) The Supplier shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account - [Details in ANNEX 3].

(3) The Technical and Organizational Measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

§4 RECTIFICATION, RESTRICTION AND ERASURE OF DATA

(1) The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Client, but only on documented instructions from the Client. Insofar as a Data Subject contacts the Supplier directly concerning a rectification, erasure, or restriction of processing, the Supplier will immediately forward the Data Subject’s request to the Client.

(2) Insofar as it is included in the scope of services, the erasure policy, ‘right to be forgotten’, rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Client without undue delay.

§5 QUALITY ASSURANCE AND OTHER DUTIES OF THE SUPPLIER

In addition to complying with the rules set out in this DPA, the Supplier shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Supplier ensures, in particular, compliance with the following requirements:

a) Appointed Data Protection Officer of the Supplier, who performs his/her duties in compliance with Articles 38 and 39 GDPR. The Data Protection Officer appointed by Supplier and of the Client (if any) are named in ANNEX 1. The Client shall be informed immediately of any change of Data Protection Officer.

b) Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Supplier entrusts only such employees with the data processing outlined in this DPA who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Client, which includes the powers granted in this DPA, unless required to do so by law.

c) Implementation of and compliance with all Technical and Organizational Measures necessary for this DPA in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR [details in ANNEX 3].

d) The Client and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.

e) The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this DPA. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of this.

f) Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with this DPA data processing by the Supplier, the Supplier shall make every effort to support the Client.

g) The Supplier shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

h) Verifiability of the Technical and Organizational Measures conducted by the Client as part of the Client’s supervisory powers referred to in Section 7 of this DPA.

§6 SUBCONTRACTING

(1) Subcontracting for the purpose of this DPA is to be understood as meaning services which relate directly to the provision of the Client service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Supplier shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

(2) Current sub-processors and Notification of new/amended sub-processors.

The Supplier may commission sub-processors (additional processors) only after prior explicit written or documented consent (textform, e-mail) from the Client. The Client hereby agrees to the commissioning of the sub-processors and their sub-processors named in ANNEX 2 on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR. The Client further grants the Supplier and its sub-processors named in ANNEX 2 the general permission to use further sub-processors. The Supplier shall inform the Client by active notification in textform - e.g. by e-mail, if he intends to engage further sub-processors or to replace sub-processors. The Client may object to such changes, but this may not be done without important data protection reasons. Objection to the intended amendment must be lodged in writing to the Supplier within 14 calendars days of notification of the amendment being made available to the contact address stated in ANNEX 2.

If no objection has been raised within 14 calendar days after notification was made to Client, Client is deemed to have authorized the new sub-processor. In case of an objection, the Parties agree to discuss commercial reasonable alternative solutions in good faith. If the parties cannot reach a resolution within sixty (60) days, Client may suspend the affected services of this DPA or terminate this DPA with a notice period of one month in writing. Such termination will be without prejudice to any fees paid or incurred by Client prior to suspension or termination and does not oblige the Supplier to any refund.

(3) The transfer of personal data from the Client to the sub-processor and the sub-processors commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved. The Supplier shall grant the Client the right to obtain information on the essential content of the contract and the implementation of the obligations of this contract, whereby the Supplier may make this dependent on the sub-processor enabling this, for example by concluding a confidentiality agreement.

(4) If the sub-processor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with the GDPR by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

§7 SUPERVISORY POWERS OF THE CLIENT

(1) If and to the extent that provision of evidences of Suppliers’ compliance with its obligations do not provide sufficient information to the Client, the Client has the right, after consultation with the Supplier, to carry out inspections or to have them carried out by an external auditor which is not a competitor of the Supplier and statutory bound to confidentiality to be designated in each individual case subject to following conditions:

a) upon prior notice of ten (10) working days (in urgent cases or upon order by a public authority even without prior notice)

b) Client requests access only during normal business hours of Client and inspections occur no more than once annually;

c) Client restricts its findings to only data relevant to Client;

d) Client avoids any disruption to the normal operations of Supplier business;

e) Client warrants, to the extent permitted by law, to keep confidential any information gathered that, by its nature, should be confidential.

(2) The Supplier shall ensure that the Client is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR. The Supplier undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

(3) Evidence of such measures, which concern not only this specific DPA, may be provided by

- Compliance with approved Codes of Conduct pursuant to Article 40 GDPR;
- Certification according to an approved certification procedure in accordance with Article 42 GDPR;
- Current auditor’s certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor)
- A suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI)) or ISO/IEC 27001).

(4) An on-site inspection at the sub-processor’s premises (if any) shall be carried out exclusively by the Supplier and at most at annual intervals under the same conditions as in Section 7 (1)) of this DPA.

(5) The Supplier may demand appropriate remuneration, to be agreed in advance with the Client in each individual case, for additional expenditure incurred as a result of his support services in connection with enabling Client inspections which are not included in the service description or which go beyond the statutory obligations of the Supplier or are not attributable to misconduct on the part of the Supplier.

§8 COMMUNICATION IN THE CASE OF INFRINGEMENTS BY THE SUPPLIER

(1) The Supplier shall reasonably assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.

b) The obligation to report a personal data breach immediately to the Client

c) The duty to assist the Client with regard to the Client’s obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.

d) Supporting the Client with its data protection impact assessment

e) Supporting the Client with regard to prior consultation of the supervisory authority

(2) The Supplier may claim compensation for support services which are not included in the description of the services, or which go beyond its statutory obligations or which are not attributable to failures on the part of the Supplier.

§9 AUTHORITY OF THE CLIENT TO ISSUE INSTRUCTIONS

(1) The Client shall immediately confirm oral instructions (at the minimum in text form).

(2) The Supplier shall inform the Client immediately if he considers that an instruction violates data privacy laws. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

§10 DELETION AND RETURN OF PERSONAL DATA

(1) Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the Main Contract, the Supplier shall hand over to the Client or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request. Unless otherwise agreed in writing, Client hereby instructs Supplier and its Sub-processors to delete all remaining data (including existing copies) from Sub-processors systems at the end of the of the contracted work in accordance with applicable law. After a recovery period of up to 30 days from that date, Supplier and/or its Sub-processors will comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days unless applicable law requires storage.

(3) Documentation which is used to demonstrate orderly data processing in accordance with this DPA shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods. It may hand such documentation over to the Client at the end of the duration to relieve the Supplier of this contractual obligation.

§11 LIABILITY

(1) The Supplier shall be liable for the proper execution of this DPA in accordance with the statutory provisions, in particular in accordance with Article 82 (2) of the GDPR. If data subjects assert claims against the Client due to unlawful or incorrect data processing, the Supplier shall support the Client and demonstrate that the Supplier has complied with its obligations specifically imposed on it as a Processor pursuant to the GDPR when processing data or has acted in compliance with the lawfully issued instructions of the Client or has not acted contrary to such instructions.

(2) In the event of breaches of this DPA caused by slight negligence, the Supplier's liability in the internal relationship with the Client shall be limited as stated in the section "Liability / Limitation of Liability" of the Main Contract; insofar as no limitation of liability has been agreed in this respect in the Main Contract, the liability of Supplier shall be limited to a total of up to a maximum of € 500,000 for all damages arising from this DPA - insofar as permissible. Liability for loss of profit, expected savings or consequential damages is excluded, with the exception of willful misconduct and gross negligence. These aforementioned limitations of liability shall also apply to vicarious agents and assistants of the Supplier.

§12 MISCELLANEOUS

(1) Unless otherwise defined herein, any words in capitalized letters herein shall have the meaning defined in the GDPR or in other applicable laws.

(2) Waiver, Amendment, Assignment. Any amendment or addition of this DPA must be in writing and signed by both Parties. Neither Party may assign, transfer, or sublicense any portion of its interests, rights, or obligations under this DPA by written agreement, merger, consolidation, change of control, operation of law, or otherwise, without the prior written consent of the other Party.

(3) Neither Party will be deemed to have waived any of its rights under this DPA by lapse of time or by any statement or representation other than by a written waiver by a duly authorized representative. No waiver of a breach of this DPA will constitute a waiver of any prior or subsequent breach of this DPA.

(4) Severability. If any provision of this DPA is held by a court of competent jurisdiction to be contrary to law, the provision shall be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of the DPA shall remain in effect.

(5) Governing Law. This DPA is governed by the laws of Germany excluding (a) its conflicts or choice of law rules, and (b) the United Nations Convention on Contracts for the International Sale of Goods. Except for a request by a Party for injunctive or other equitable relief, any dispute arising out of this DPA will be subject to the exclusive jurisdiction of the courts of Düsseldorf, Germany.

(6) Rule of Precedent. In the event of any conflict or inconsistency between the Main Contract and this DPA regarding the subject matter of this DPA the following rule of precedence shall apply to the extent possible by applicable law: 1. this DPA 2. the Main Contract.

CLIENT	**SUPPLIER**
[Place], [Date] CGI Deutschland B.V. & Co. KG	[Place], [Date] [CGI Legal Entity Name]
[Name]	[GF, ppa. / i.V. / i.A.] [Name]
[Name]	[GF, ppa. / i.V. / i.A.] [Name]

ANNEXES

ANNEX 1 – DATA PROCESSING SCHEDULE

This ANNEX specifies and documents the Suppliers’ processing activities (as Data Processor) relevant to the Main Contract on behalf of the Client (as Data Controller).

1. SUBJECT MATTER AND PURPOSE

The Data Processor shall process the Personal Data in order to:	The application called "Door James" is a member registration tool which stores and processes identity and contact data of Controllers employees and visitors as well as login data within the framework of respective Back2Office guidelines.

2. CATEGORIES OF DATA SUBJECTS

The Personal Data comprises the following Data Subjects:	☐ Customers ☐ Potential Customers ☐ Subscribers ☒ Employees of Controller/its Customers (employees, working students, trainees, apprentices) ☐ Suppliers / Service Providers of Controller ☐ Cooperation Partners / Contractual Partners ☐ Contact Persons ☐ Other: (Please specify)

3. CATEGORIES OF PERSONAL DATA

The Data Processor shall process Personal Data comprising the following data types/categories	☒ Identity and contact data (Name, address, Telephone, e-mail address, Birthdate etc) ☐ Contract Data (Contractual/Legal Relationships, Contract or Product Interest) ☐ Economic and Financial Data (Contract Billing, Payments Data, Bank Accounts, Creditcard No., credit rating, payment history, balances etc.) ☐ IT user data, Login, Traffic, and Audit/Tracking Data ☐ Professional Life Data ☐ Private Life Data ☐ Demographic Data ☐ Location Data ☐ Other: (Please specify)

4. SENSITIVE CATEGORIES OF PERSONAL DATA

Data Processor shall process one or more of the listed categories of sensitive Personal Data (please specify)	☐ Racial or ethnic origin ☐ Political opinions ☐ Religious or philosophical beliefs ☐ Trade union membership ☐ Biometric data for the purpose of uniquely identifying a natural person ☐ Genetic data ☐ Data concerning a person’s physical or mental health ☐ Data concerning a person’s sex life or sexual orientation ☐ Criminal convictions or intelligence of or of any offences alleged to have been committed ☒ Other:**Validity date of a person’s vaccination, recovery or Covid19 test status**

5. NATURE OF THE PROCESSING

In the course of processing by the Data Processor, personal data inter alia, shall be:	☒ collected ☒ recorded ☐ organized / arranged ☒ stored ☐ adapted / modified ☒ read ☐ queried ☐ used ☒ disclosed ☐ synchronized ☒ combined / linked ☐ restricted ☒ deleted ☐ destroyed

6. CONTACT DETAILS OF DATA PROTECTION OFFICERS (IF APPOINTED)

Name and contact details of the Client’s Data Protection Officer	Klicken oder tippen Sie hier, um Text einzugeben.
Name and contact details of the Processors’ Data Protection Officer	Burkhard Grün datenschutz.de@cgi.com CGI Deutschland B.V. & Co. KG Datenschutzbeauftragter – personal/confidential- Leinfelder Str. 60, 70771 Leinfelden-Echterdingen

ANNEX 2 – APPROVED SUB-PROCESSORS AND APPROPIATE GUARANTEES

Data Controller authorizes that the Data Processor may appoint/has appointed the following Sub-processors for the Processing of the Personal Data:

name of legal entities	Categories of data transferred	Purpose for data transfer	Location of Sub-processor
Google Commerce Limited, including all Google Sub-processors listed under https://cloud.google.com/terms/sub-processors https://cloud.google.com/terms/third-party-suppliers as may be updated by Google from time to time in accordance	**All categories mentioned in ANNEX 1 3. CATEGORIES OF PERSONAL DATA**	**Hosting services,** https://cloud.google.com/privacy/gdpr	Dublin, Ireland and any country in which Google or its Sub-processors maintain facilities.
Twilio Inc.	**All categories mentioned in ANNEX 1 3. CATEGORIES OF PERSONAL DATA**	**E-Mail Services,** https://www.twilio.com/legal/data-protection-addendum	San Francisco, USA
Mongodb Limited	**All categories mentioned in ANNEX 1 3. CATEGORIES OF PERSONAL DATA**	**Database services,** https://www.mongodb.com/cloud/trust/compliance/gdpr	Dublin, Ireland

Further outsourcing by a Sub-processor

☐ Is not permitted;

☐ Requires the express consent of the main Client (at the minimum in text form);

☒ Requires the express consent of the Supplier (at the minimum in text form);

All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional Sub-processor.

TRANSFER OF DATA TO A COUNTRY OUTSIDE EU/EEA AND APPROPRIATE SAFEGUARDS OF ART 44 ET SEQ. GDPR

Country/ Supplier/ Sub-processor	**Adequacy decision** of European Commission (Article 45 Paragraph 3 GDPR);	**Binding Corporate Rules** (Article 46 Paragraph 2 Point b in conjunction with Article 47 GDPR);	**Standard Data Protection Clauses** (Article 46 Paragraph 2 Points c and d GDPR);	**Approved Codes of Conduct** (Article 46 Paragraph 2 Point e in conjunction with Article 40 GDPR);
Google (Irland)	☐	☐	☒	
Twilio (USA)	☐	☒	☐	
MongoDB Atlas (Irland)	☐	☐	☒	

CONTACT ADDRESS FOR OBJECTIONS TO NEW/AMENDED SUB-PROCESSORS

Name	**E-mail Address**
Fabian Rüter	**Fabian.rueter@cgi.com**

ANNEX 3 – Technical and Organizational Measures

1. Confidentiality (Article 32 Paragraph 1Point b GDPR)

- Physical Access Control
  No unauthorised access to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems
- Electronic Access Control
  No unauthorised use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media
- Internal Access Control (permissions for user rights of access to and amendment of data)
  No unauthorised Reading, Copying, Changes or Deletions of Data within the system, e.g. rights authorisation concept, need-based rights of access, logging of system access events
- Isolation Control
  The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Client support, sandboxing;
- Pseudonymisation (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR)
  The processing of personal data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and Organizational measures.

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

- Data Transfer Control
  No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;
- Data Entry Control
  Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management

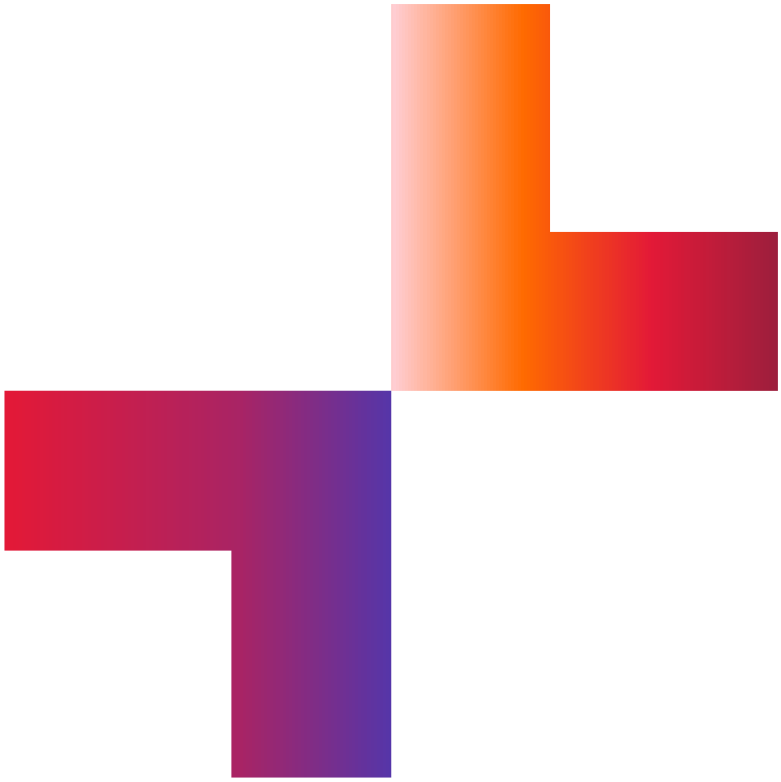
3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

- Availability Control
  Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning
- Rapid Recovery (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR);

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

- Data Protection Management;
- Incident Response Management;
- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);
- Order or Contract Control
  No third party data processing as per Article 28 GDPR without corresponding instructions from the Client, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.

. . . . . .



de.cgi.com