Data Protection Agreement (DPA) for the performance of security assessments, security monitoring and forensic investigations

between

Customer (hereinafter referred to as "CUSTOMER")
street
place
Switzerland

and

Compass Security Schweiz AG (hereinafter referred to as "COMPASS")
P.O. Box 2038
Werkstrasse 20
CH-8640 Rapperswil
Switzerland

1 Data Protection Agreement

1.1 Preamble

COMPASS shall carry out security, test and inspection work for the CUSTOMER in accordance with the "Service Agreement" existing between these parties. In doing so, IT systems are tested for security and vulnerabilities on behalf of the CUSTOMER. It is possible that, whilst carrying out these services, COMPASS will get in contact with personal data controlled by the CUSTOMER.

The parties therefore state that, depending on the Jurisdiction of the CUSTOMER, the EU Regulation 2016/679 (General Data Protection Regulation "GDPR") or the Swiss Federal Act on Data Protection ("FADP" together with GDPR "Data Protection Laws") might be applicable to this contractual relationship. Therefore, the parties agree that a possible, but unintended, processing of personal data is based on this data protection agreement ("DPA") which takes the provisions of the Data Protection Laws into account.

1.2 Subject matter

The data processing activities conducted by COMPASS result from the Service Agreement between the CUSTOMER and COMPASS.

Within the scope of the investigations and testing activities, attempts are being made to attack the system(s) of the CUSTOMER or to analyze compromised systems. COMPASS will try to find and identify vulnerabilities in the system and the corresponding organization. CUSTOMER data will be accessed and analyzed. Due to the nature of these activities, several types of data might be intentionally or accidentally accessed, this might include personal data.

The "Service Agreement" as well as this data protection agreement do not contain an explicit order from the CUSTOMER for the processing of personal data according to Art. 4 and 28 GDPR (Art. 5 and Art. 9 FADP) by COMPASS.

However, it is nevertheless possible that personal data according to the definition of Art. 4 GDPR (Art. 5 FADP) might be processed. For this reason, the potential processing of this data and the relationship between CUSTOMER and COMPASS is regulated in this Data Processing Agreement according to Art. 28 DS-GVO (Art. 9 FADP).

The CUSTOMER explicitly acknowledges that COMPASS may process personal data within the scope of the performance of the services.

1.3 Duration

The duration of this contract corresponds to the duration of the "Service Agreement".

1.4 Description of Service

The subject of the service delivered is described in detail in the "Service Agreement", see chapter "Project description".

Nature and purpose of processing: The contractor provides IT security and penetration tests, security monitoring, digital forensics or incident response for the client and may process personal data of the client in this context in accordance with the CUSTOMERS' instructions. Due to the nature of the "Service Agreement", it is not possible to make any statements about personal data that may be processed before the order is executed.

Type of personal data: The personal data which may be processed is that which is located in the CUSTOMER environment. This may include but is not limited to the name and contact details of employees, customers and members of the CUSTOMER.

It is also possible that special categories of personal data pursuant to Art. 9 GDPR (or as defined in Art. 5 FADP) might be accessed or processed by COMPASS. The CUSTOMER confirms that in this case he has fulfilled his obligations towards these data subjects in accordance with the Data Protection Laws.

If special categories of personal data might be processed or accessed, CUSTOMER shall inform COMPASS prior to the execution of the order and instruct "Compass" which measures are to be taken.

Categories of data subjects: In particular, employees of the CUSTOMER, its customers and members may be affected by the processing.

1.5 Technical / organizational measures

COMPASS shall ensure that any personal data which it may receive is adequately protected (see Appendix 1).

1) COMPASS shall provide security pursuant to Art. 28,32 GDPR (Art. 8,9 FADP), in particular in conjunction with Art. 5 GDPR (Art. 6 FADP). Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity and availability of the systems. The state of the art, the implementation costs and the type, scope and purpose of the processing as well as the different probability of occurrence and severity of the risk for the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR (Art. 8 FADP) must be taken into account (details in Appendix 1).

2) COMPASS shall document the implementation of the technical and organizational measures outlined prior to the commencement of the processing and shall hand them over to the CUSTOMER for review upon request (see Appendix 1). By signing this agreement, the documented measures in accordance with Appendix 1 become the basis of the order. If the inspection or an audit of the CUSTOMER reveals a need for adjustment, this shall be implemented by mutual agreement.

3) The technical and organizational measures are subject to technical progress and further development. In this respect, COMPASS is permitted to implement alternative measures. In this case, the security level defined may not be undercut. Material changes must be documented.

1.6 Processing of data and data subjects' rights

1) COMPASS has no explicit mandate to process personal data. Within the scope of security investigations, however, it is possible for personal data to be accessed, collected and temporarily stored for the duration of the contract or as defined under the Service Agreement by COMPASS. This data is used for documentation of the test results and to control the test procedure. Any further processing is excluded.

2) COMPASS shall immediately delete personal data which is not required for the execution of the test activities or their evaluation and documentation. Alternatively, COMPASS may anonymize this data.

3) All data subjects' rights must be asserted with the CUSTOMER. COMPASS shall not provide any direct information to data subjects. COMPASS does not give any information about the existence or content of the order or the contents of the "Service Agreement".

1.7 Quality assurance and other obligations of COMPASS

In addition to compliance with the provisions of this order, COMPASS shall have statutory obligations pursuant to the GDPR or FADP; to this extent, COMPASS shall in particular guarantee compliance with the following requirements:

1) Maintaining confidentiality pursuant to Art. 28 para. 3 sentence 2 lit. b, Art. 29, 32 para. 4 GDPR (Art. 8 FADP). When carrying out the work, COMPASS shall only employ employees who are obliged to maintain confidentiality and who have received adequate data privacy training. COMPASS and any person subordinate to COMPASS who has access to personal data may only process this data in accordance with the instructions of the CUSTOMER, including the powers granted in the "Service Agreement" and this data protection agreement, unless COMPASS is legally obliged to process this data.

2) The implementation of and compliance with all technical and organizational measures required for this order pursuant to Art. 28 para. 3 sentence 2 lit. c, 32 GDPR (details in Appendix 1) (Art.7 FADP).

3) Insofar as the CUSTOMER is subject to inspection by the supervisory authority, administrative offence or criminal proceedings, the liability claims of a data subject or a third party or any other claim in connection with data processing activities undertaken by COMPASS in relation to the performance of the services, COMPASS shall support the CUSTOMER to the best of its ability.

4) COMPASS shall regularly monitor the internal processes as well as the technical and organizational measures to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable Data Protection Laws and that the rights of the data subject are protected.

5) Grant the verifiability of the technical and organizational measures within the scope of the control powers of the CUSTOMER in accordance with section 1.9 of this agreement.

6) As a rule, COMPASS cannot maintain a processing directory in accordance with Art. 30 GDPR (Art. 12 FADP) due to the unknown content of the test data.

Data protection officer:

Dr. Sarah Weiss
Paulstrasse 13
DE-67346 Speyer
Tel. +49 623 23185490
Mail: privacy@compass-security.com

1.8 Subcontracting

1) For the purposes of this regulation, subcontracting shall mean services which relate directly to the provision of the principal service. This does not include ancillary services used by COMPASS e.g. as telecommunications services, postal/transport services, maintenance and user services or the disposal of data carriers as well as other measures to ensure confidentiality, availability, integrity of the hardware and software of data processing systems. However, COMPASS shall be obliged to take appropriate contractual agreements and control measures to ensure the data protection and data security of the CUSTOMER's data even in the case of outsourced ancillary services.

2) COMPASS shall inform CUSTOMER of any intended change regarding the involvement of new subcontractors or the replacement of existing subcontractors, which gives the Controller the opportunity to object to such changes (Art. 28 para. 2 sentence 2 GDPR). The subcontractors listed in Appendix 3 shall be deemed approved.

3) The passing on of the CUSTOMER's personal data to a subcontractor is only permitted when all requirements for subcontracting have been met.

4) If the subcontractor yields the agreed service outside the EU/EEA, COMPASS shall ensure that it is permissible under data protection law by taking appropriate measures. The same applies if services within the meaning of para. 1 sentence 2 are to be used. An appropriate level of data protection was established by the EU Commission in a formal decision for Switzerland: 2000/518/EC (although this is a dated adequacy decision, it was confirmed to be still in force 12/2024).

1.9 Control rights of the CUSTOMER

1) CUSTOMER shall have the right, in consultation with COMPASS, to carry out audits or to have them carried out by auditors to be appointed in individual cases. CUSTOMER has the right to assess the compliance of COMPASS with this agreement by means of audits, which need to be announced in advance.

2) COMPASS shall ensure that the CUSTOMER can verify the compliance of COMPASS with this agreement. COMPASS delivers to the CUSTOMER the necessary information upon request.

3) The proof of compliance can be provided by

   a) Direct audit by the CUSTOMER;
   b) compliance with approved rules of conduct pursuant to Art. 40 GDPR (Art. 11 FADP);
   c) certification in accordance with an approved certification procedure pursuant to Art. 42 GDPR (Art. 13 FADP);
   d) compliance with binding data protection regulations within the group in accordance with Art. 47 GDPR (Art. 15, para 2 lit 4);
   e) audit reports or report extracts from independent bodies (e.g. auditors, audit, data protection officer, IT security department, data protection auditors, quality auditors);
   f) a suitable certification by an IT security or data protection body;
   g) If unexpected costs result from an inspection or providing the required evidence, COMPASS may demand reasonable compensation from the CUSTOMER.

1.10 Notification of data breaches (Data Breach Notification)

1) COMPASS shall support the CUSTOMER in complying with the obligations set out in Articles 32 to 36 of the GDPR (Art. 8, 22 - 24 FADP) regarding the security of personal data, reporting obligations in the event of data breakdowns, data protection impact assessments and prior consultations.
   These include, but are not limited to

   a) notification that personal data could have been compromised
   b) ensuring an adequate level of protection through technical and organizational measures which take into account the circumstances and purposes of the processing and the predicted likelihood and severity of a potential breach of rights through security breaches, thus enabling relevant breaches to be identified on an ongoing basis
   c) the obligation to report violations of personal data to the CUSTOMER without undue delay

d) the obligation to assist the CUSTOMER in fulfilling its obligation to inform the person concerned and to provide him with all relevant information in this connection
e) assisting the CUSTOMER in its data protection impact assessment
f) assisting the CUSTOMER in prior consultations with the supervisory authority

2) COMPASS may claim reasonable compensation for costs incurred by the CUSTOMER in exercising his rights of control and providing the required supporting documents.

1.11 Authority of the CUSTOMER to issue instructions

1) Oral instructions are confirmed by both parties without delay (at least in text form).

2) COMPASS must inform the CUSTOMER immediately if instructions might violate data protection regulations. COMPASS is entitled to suspend the execution of the corresponding instruction until it has been confirmed or changed by the CUSTOMER.

1.12 Deletion and return of personal data

1) Copies or duplicates of the data will not be made without the knowledge of the CUSTOMER. Excluded from this are backup copies insofar as they are necessary to guarantee proper data processing, as well as data which are necessary regarding compliance with archiving or data retention obligations.

2) Data necessary for the documentation of the inspection and the traceability of the work shall be stored for as long as is necessary for the respective order. CUSTOMER may demand that data be deleted after completion of the inspection. COMPASS shall carry out the deletion. Data will be deleted 5 years after completion of the check without comprehensible instructions from the CUSTOMER.

3) Upon completion of the contractually agreed work or earlier upon request by the CUSTOMER - at the latest upon termination of the "Service Agreement" - COMPASS must hand over to the CUSTOMER all documents, processing and usage results created as well as data in connection with the contractual relationship which have come into his possession or, after prior consent, destroy them in accordance with data protection regulations. The same applies to test data. The protocol of the disposal/deletion must be submitted upon request.

4) Documentation which serves as proof of fulfilling these statutory and/or other applicable obligations shall be kept by COMPASS in accordance with the respective retention periods beyond the end of the performance agreement. COMPASS may hand them over to the CUSTOMER at the end of the contract for his relief.

1.13 Final provisions

1) This agreement does not replace any previous agreements.

2) Subsidiary agreements or amendments to this order must be made in writing.

3) References to laws, regulations, documents and appendices shall apply to the laws, regulations, documents and appendices in their respective valid versions, i.e. including any amendments after the date of this agreement, unless expressly provided otherwise.

4) The Appendices are an integral part of this Agreement. In the event of a contradiction between the provisions of the actual agreement text and its appendices, the provisions of the agreement shall prevail. Mandatory legal regulations, however, remain unaffected.

5) Should individual provisions of this order be or become invalid or unenforceable, this shall not affect the validity of the remaining parts. In such a case, the parties undertake to replace the invalid or unenforceable provision with a provision that comes as close as possible to the intended purpose in a legally permissible manner; the same shall apply in the event of gaps. In the event of a contradiction between data protection-relevant contents of this data protection agreement with the "Service Agreement" or the general terms and conditions, the provisions of this agreement take precedence.

6) The CUSTOMER confirms that he is the controller and therefore complies with the provisions of the applicable data protection laws. Furthermore, the CUSTOMER does not offer any content for processing which could constitute a violation of the personal rights of the data subjects.

7) In the external relationship, the CUSTOMER shall be liable in accordance with the data protection liability provisions for the damage caused by processing that does not conform to the law. COMPASS is only liable for the damage caused by a processing if it has not fulfilled its obligations under this agreement or acted against the instructions of the CUSTOMER. The liability provisions of the performance agreement and the general terms and conditions shall apply.

Appendix 1

Technical / Organizational measures

1. Confidentiality

- Access Control

  No unauthorized access to data processing equipment:

  ☐ Magnetic or chip cards

  ☒ Keys

  ☐ Electric door openers

  ☐ Security guard or doormen

  ☒ Alarm systems

  ☐ Video systems

  ☐ Automatic access control system

  ☒ Locking system with code lock

  ☒ Manual locking system

  ☐ Safety locks

  ☒ Key policy

  ☐ Logging of visitors

  ☒ Careful selection of cleaning personnel

  ☐ Careful selection of security personnel

  ☐ Obligation to wear authorization cards

  ☒ Visitors are supervised

  ☒ Everyone knows everyone

- Access Control

  No unauthorized system usage:

  ☒ Secure passwords

  ☒ Automatic lock mechanisms

  ☒ Two-factor authentication

  ☒ Encryption of data carriers

  ☒ Assignment of user rights

  ☒ Creating user profiles

  ☒ Authentication with username / password

  ☐ Housing interlocks

  ☒ Use of VPN technology

  ☐ Locking of external interfaces (USB etc.)

  ☒ Encryption of mobile data media

  ☐ Encryption of smartphone content

  ☐ Use of central smartphone administration software

☒ Use of anti-virus software

☒ Encryption of data carriers in laptops / notebooks

☒ Use of a hardware/software firewall

- Access Control

  No unauthorized reading, copying, modification or removal within the system

  ☒ Authorization concepts and demand-oriented access rights

  ☒ Logging of accesses

  ☒ Creating an Authorization Concept

  ☒ Administration of rights by system administrator

  ☒ Reduction of the number of administrators

  ☒ Password policy incl. password length, password change

  ☒ Secure storage of data media

  ☒ Secure wiping of data media before reuse

  ☒ Proper destruction of data carriers (DIN 66399)

  ☒ Encryption of data carriers

- Separation Control

  Separate processing of data collected for different purposes:

  ☒ Sandboxing

  ☒ Physically separate storage on separate systems or data carriers

  ☒ Software-based client separation

  ☒ Creation of an authorization concept

  ☐ Encryption of data sets processed for the same purpose

  ☐ For pseudonymized data: Separation of the assignment file

  ☒ Definition of database rights

- Pseudonymization (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)

  ☐ The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the involvement of additional information, provided that this additional information is kept separately and is subject to appropriate technical and organizational measures.

2. Integrity

- Handover control

  No unauthorized reading, copying, modification or removal during electronic transmission or transport

  ☒ Encryption

  ☒ Virtual Private Networks (VPN)

  ☒ Digital Signature

  ☒ Passing on personal data in anonymous or pseudonymous form

  ☐ Creating an overview of regular retrieval and transmission processes

  ☐ Documentation of the recipients of data and the time spans of the planned transfer or agreed deletion periods

  ☐ During physical transport: secure transport containers/packaging

- Input Control

  Determine whether and by whom personal data have been entered into, modified in or removed from data processing systems:

  ☐ Recording of the input, modification and deletion of personal data

  ☒ Document management

  ☒ Create an overview of which applications can be used to enter, change and delete which personal data

  ☒ Traceability of input, modification and deletion of personal data by individual usernames

  ☐ Storage of forms from which personal data have been transferred to automated processing operations

  ☒ Allocation of rights to enter, change and delete personal data on the basis of an authorization concept

3. Availability and resilience

- Availability Control

  Protection against accidental or deliberate destruction or loss:

  ☒ Backup strategy (online/offline; on-site/off-site)

  ☒ Uninterruptible power supply (UPS)

  ☒ Virus protection

  ☒ Firewall

  ☒ Reporting routes and contingency plans

  ☒ Rapid recoverability (Art. 32 para. 1 lit. c DS Block Exemption Regulation)

  ☒ Air conditioning in server rooms

  ☒ Protective socket strips in server rooms

  ☒ Fire and smoke detection systems

  ☒ Alarm message in case of unauthorized access to server rooms

  ☒ Creating a backup concept

  ☒ Storage of data backup at a secure, outsourced location

4. Procedures for regular review, assessment and evaluation

- Data Protection Management;
- Incident-Response-Management;
- Data protection-friendly default settings / privacy by design (Art. 25 para. 2 GDPR);
- Order Control

  No order data processing within the meaning of Art. 28 GDPR without corresponding instructions from the client:

  ☒ Unambiguous contract design

  ☐ Formalized order management

  ☒ Strict selection of the service provider

  ☐ Obligation of prior conviction

  ☒ Follow-up checks

Appendix 2

Additional clauses for processing of personal data to which the Federal Act on Data Protection, Switzerland, applies

1) "Personal data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the meaning assigned to them by the Swiss Federal Act on Data Protection (Loi fédérale sur la protection des données; Datenschutzgesetz) including the relevant amendments or revisions and its implementing ordinances (whereby "the authority" shall mean the competent data protection authority in the territory in which the data CUSTOMER is established).

2) The competent supervisory authority for data processing activities where the Federal Act on Data Protection applies shall be the Federal Data Protection and Information Commissioner (FDPIC), in Switzerland.

Appendix 3

Subcontractors

Unless otherwise stipulated in the individual contract, subcontractors are:

1) Compass Security Deutschland GmbH

2) Compass Security Cyber Defense AG

3) Compass Security Network Computing AG

4) Compass Security (Canada) Network Computing Inc.

The regulatory obligations apply to all subcontractors.

Communication

COMPASS uses Microsoft Software and the M365 services from Microsoft to process data and for communication (MS Teams, MS Exchange Online, MS SharePoint and more). According to current information from Microsoft, all data is stored on servers in Switzerland. Details of the products and the conditions applicable can be found here: https://www.microsoft.com/licensing/terms/product/ForallSoftware/all.

By using Microsoft Cloud products, CUSTOMER accepts the Microsoft product and licensing terms as well as the data protection and security terms. The CUSTOMER understands that Microsoft terms and conditions are subject to change at any time. The Microsoft Terms of Use and Privacy Policy for protecting data in the Microsoft Cloud can be found here: https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/all (Microsoft Privacy and Security Terms).

A comprehensive, service-dependent security concept ensures that data cannot be inadvertently placed in the Microsoft Cloud by COMPASS. Organizational and technical measures ensure that no confidential customer data is stored in the MS Cloud. The security concept can be inspected by CUSTOMER at any time if required, given the applicable confidentiality agreements have been signed beforehand.

Server Housing

As part of the service, the CUSTOMER's data may be hosted on servers of COMPASS located in the datacenter of the third-party provider Green Datacenter AG (Industriestrasse 33, 5242 Lupfig, Switzerland) in Switzerland. The datacenter is a provider with a strong commitment to data protection and security. In the server housing, the data center generally has no access to any data.

For emergency situations requiring physical intervention, COMPASS has entered into a remote hands agreement with the datacenter to provide on-site support. Such access is strictly limited to non-sensitive operational tasks and is carried out under the guidance of COMPASS. All data received as part of the service will be encrypted both in transit and at rest using industry standard encryption protocols.

COMPASS has signed contracts in accordance with data protection laws and ensures that the datacenter meets strict security standards and complies with applicable data protection laws to ensure the confidentiality, integrity and availability of the CUSTOMER's data at all times.