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

between

the Customer, who is mentioned in the individual contract among Contracting Parties	(hereinafter referred to as "CUSTOMER")

and

Compass Security Schweiz AG P.O. Box 2038 Werkstrasse 20 CH-8645 Jona Schweiz	(hereinafter referred to as "COMPASS")

1 Data Protection Agreement

1.1 Preamble

COMPASS shall carry out 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. No personal data will be processed on behalf of the CUSTOMER, but it is possible that personal data of the CUSTOMER or his employees, business partners etc. could be accessed.

The parties therefore state that the EU Regulation 2016/679 (General Data Protection Regulation "GDPR") 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 GDPR into account.

1.2 Subject matter

The subject matter of the order results from the individual contract 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 analyse compromised systems. COMPASS will try to find and identify vulnerabilities in the system and the corresponding organisation. CUSTOMER data will be accessed and analysed. Due to the nature of these activities, several types of data might be intentionally or accidentally be accessed, this might include personal data.

The „Service Agreement“ as well as this data protection agreement do not contain an explicit order of the CUSTOMER for the processing of personal data according to Art. 4 and 28 GDPR by COMPASS.

However, it is nevertheless possible that personal data according to the definition of Art. 4 GDPR might be processed. For this reason, the potential processing of this data and the relationship between CUSTOMER and COMPASS has been regulated in this Data Processing Agreement.

The CUSTOMER explicitly acknowledges that COMPASS may unintentionally process personal data.

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".

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.

It is also possible that special categories of personal data pursuant to Art. 9 GDPR 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 GDPR.

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.

1.5 Technical / organisational measures

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

1) COMPASS shall provide the security pursuant to Art. 28 para. 3 lit. c, 32 GDPR, in particular in conjunction with Art. 5 para. 1, para. 2 GDPR. 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 must be taken into account (details in Annex 1).

2) COMPASS shall document the implementation of the technical and organisational measures outlined prior to the commencement of the processing and shall hand them over to the CUSTOMER for review upon request (see Annex 1). By signing this agreement, the documented measures in accordance with Annex 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 organisational 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) In principle, COMPASS does not carry out any processing of personal data as defined in the GDPR. COMPASS has no explicit mandate to process personal data. Within the scope of security investigations, however, it is possible for personal data to be collected and stored by employees of COMPASS. This data is used to document 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 anonymise 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; 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, 29, 32 para. 4 GDPR. 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 these 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 organisational measures required for this order pursuant to Art. 28 para. 3 sentence 2 lit. c, 32 GDPR (details in Annex 1).

3) Insofar as the CUSTOMER is subject to inspection by the supervisory authority, administrative offence or criminal proceedings, the liability claims of a person concerned or a third party or any other claim in connection with order processing at COMPASS, 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 organisational measures to ensure that the processing in the area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the rights of the data subject are protected.

5) Grant the verifiability of the technical and organisational measures within the scope of the control powers of the CUSTOMER in accordance with section 8 of this agreement.

6) As a rule, COMPASS cannot maintain a processing directory in accordance with Art. 30 GDPR 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 the 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 may only commission subcontractors (further contract processors) with the prior express written or documented consent of the CUSTOMER.

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.

COMPASS uses M365 services from Microsoft to process data and for communication (MS Teams, MS Exchange, SharePoint). 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. 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 further 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.
COMPASS point out that for secure use of the M365 Cloud services, a security concept must be in place on CUSTOMER side. comprehensive protection settings must also be made on the client side (the local system under the control of CUSTOMER). CUSTOMER is responsible for adapting these protection settings to CUSTOMERs needs, data protection and security requirements.

Unless otherwise stipulated in the individual contract, subcontractors are:

- Compass Security Deutschland GmbH
- Compass Security Cyber Defense AG
- Compass Security Network Computing AG
- Compass Security (Canada) Network Computing Inc.

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;
   c) certification in accordance with an approved certification procedure pursuant to Art. 42 GDPR;
   d) compliance with binding data protection regulations within the group in accordance with Art. 47 GDPR;
   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) COMPASS may claim remuneration for costs incurred as a result of exercising the control rights and providing the required evidence.

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 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 organisational 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 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 an instruction 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 with regard to 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, unless there are compelling legal reasons for storing the data. Data will be deleted after 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 fully complies with the provisions of the GDPR and 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 / Organisational measures

1. Confidentiality (Art. 32 para. 1 lit. b DS-GVO)

- 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 authorisation 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 user name / 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 pseudonymised data: Separation of the assignment file

  ☐ Definition of database rights

- Pseudonymisation (Art. 32 para. 1 lit. a DS-GVO; Art. 25 para. 1 DS-GVO)

  ☐ 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 organisational measures.

2. Integrity (Art. 32 para. 1 lit. b DS-GVO)

- 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 user names

  ☐ 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 (Art. 32 para. 1 lit. b DS-GVO)

- 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 (Art. 32 para. 1 lit. d DS-GVO; Art. 25 para. 1 DS-GVO)

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

- Order Control

  No order data processing within the meaning of Art. 28 DS-GVO 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