Unilateral Commitment Statement

on the processing of personal data on behalf of the controller according to Data Protection Act and article 28 of General Data Protection Regulation (GDPR)

by

CANCOM Austria AG
Wienerbergstraße 53, 1120 Wien

(hereinafter „processor“)

in support of

Controller

(hereinafter „controller“),

1 Object of the Commitment

1 The Processor provides services to the Controller on the basis of a separately concluded agreement (hereinafter referred to as "Basic Agreement"), which consist of or involve the processing of personal data (hereinafter referred to as "data") within the meaning of Art. 4 fig. 1 and 2 of the EU General Data Protection Regulation (GDPR). This supplementary commitment forms the specific legal basis for the data processing pursuant to Article 28 (3) DSGVO, whereby the controller acts as the (sole) "controller" and the processor as the "processor" in this respect. Insofar the term “data processing” or “processing” (of data) is used in this Unilateral Commitment Statement (hereinafter referred to as “Commitment”), the definition of “processing” within the meaning of Article 4 (2) of the GDPR shall apply.

2 With this Commitment, the processor assures the controller and undertakes to comply with and ensure all requirements arising from Article 28 (3) GDPR for him as processor. In particular, the processor shall ensure both the compliance with the obligations set out below as well as the implementation of services in the course of the data processing relationship.

2 Qualification as processor

3 The processor constitutes a processor within the meaning of Article 28 (1) GDPR that provides sufficient guarantees that appropriate technical and organizational measures (hereinafter referred to as "TOMs") are implemented and ensured accordingly. The TOMs implemented and assured by the processor are listed in the Annex to this Commitment.

4 The processor warrants and undertakes that these TOMs are ensured for all data processing that the processor carries out for the controller. However, this shall only apply to the extent that the systems and accesses affected are located within the sphere of the processor.

5 If systems affected by the data processing are located within the sphere of the controller, the TOMs listed in the Annex are assured insofar as they are in the sphere of influence of the processor and therefore the respective TOM is applicable (explanatory example: If a server is located on the premises of the controller, the TOMs regarding access control to this server do not apply, as they are not within the sphere of influence of the processor).

6 Unless the processor is legally obliged to perform certain processing activities, controller’s data will be processed solely by the processor to fulfill its contractual obligation to the controller, i.e. as regulated herein or as instructed by the controller. The processor shall inform the controller in advance of any other legal processing obligations to the extent permissible.

7 Under no circumstances will the processor use the data for its own purposes or those of third parties or transmit data to third parties without the written instruction or consent of the controller. Copies or duplicates of data shall only be made without separate consent of the controller to the extent that they are required to ensure proper processing (backup copies) or with regard to statutory retention obligations.

8 The data shall be processed within the territorial scope of the GDPR, unless both a written authorization of the controller for a transfer to third countries and the specific requirements of Article 44 et seq. GDPR are available.

9 The data processing shall be carried out overall in a manner that supports the controller at all times in fulfilling its obligations under data privacy law towards data subjects and public authorities.

10 Upon completion of the agreed service provision (at the latest upon termination of the contract) or upon prior request by the controller, the processor shall return all information, documents, the processing and utilization results as well as the data sets related to the contractual relationship (including test and scrap material) to the controller in a common file format or destroy them after the controller's prior consent in accordance with data protection regulations.

3 Rights of the controller

11 The controller has a comprehensive right to issue instructions to the processor regarding the type and extent of data processing. If, in the opinion of the processor, such instructions could violate applicable data protection law, the processor must warn the controller without delay (Art. 28 (3), 3rd sentence of the GDPR).

12 The decision on the provision of information, restriction, deletion or correction of data records which are the subject matter of the contract shall be the exclusive responsibility of the data controller. The Processor shall never act on its own authority in this regard, but only in accordance with the documented instructions of the Controller. If data subjects contact the processor directly in this regard, the processor shall endeavour to forward such requests to the controller.

4 Obligations of the processor

13 The processor is responsible for the contractually stipulated data processing within the scope of the relevant provisions of the data protection law. The processor confirms knowledge of all relevant regulations and in particular observes the principles of proper data processing pursuant to Art. 5 GDPR.

14 The processor undertakes to process all personal data in accordance with the specifications of the controller pursuant to Art. 4 (7) GDPR and to pursue only the means and purposes specified by the controller.

15 Concrete obligations or detailed behavioural requirements that do not result directly from the basic contract or from objective law must be documented as "data processing instructions" by the data controller.

16 The processor guarantees that all persons employed or authorized for data processing are suitably qualified and have been bound to to confidentiality or are subject to an appropriate – in particular legal – duty to confidentiality (Art. 28 (3) lit b GDPR). The duty of confidentiality shall also be observed after termination of the basic agreement. The Processor expressly declares that employees concerned will be be sufficiently instructed, regularly trained or their awareness raised and provided with specific instructions and supervision with regard to data protection/information security.

17 The processor undertakes to take all measures necessary for the security of data processing, pursuant to Art. 32 GDPR. The processor will take all organizational and technical precautions to ensure the integrity of the processing, to ensure the integrity of the processing, prevent the loss of personal data and prevent unauthorized access by third parties. The measures already implemented by the processor are listed in the annex and correspond to the security concept according to ISO 27001. The certificate can be presented to the controller upon request. The processer shall regularly monitor and document his processes and the effectiveness of his measures and, if necessary, make/arrange modifications that have become necessary or are in line with the technical progress.

18 As far as possible, the processor supports the controller in the realization of his/her information requirements and the claimed rights of the persons affected (art 28 paragraph 3 lit e GDPR). In particular, the processor shall create the technical and organizational conditions for the controller to fulfil his/her obligations towards the data subjects within the relevant deadlines in accordance with art. 15 ff GDPR. In any case, the processor shall provide the controller with the information that can be obtained with a reasonable technical and economic effort.

19 The processor shall also assist the controller, taking into account the nature of the processing and the information available to the processor, in fulfilling the controller's obligations under Articles 32-36 of the GDPR (Article 28(3)(f) of the GDPR).

20 The processor shall immediately (i.e. as soon as the processor obtains knowledge of the relevant incident) inform the controller (or his/her data protection commissioner) about relevant personal data breaches and data security breaches of contractual data. In particular, the extent to which the data records/ data categories and data subjects are affected, the expected consequences of data breach, the countermeasures taken planned as well as contact details of a responsible authorized person or other contact point of the processor shall be provided for detailed information/coordination.

21 The processor shall make information available to the controller in an appropriate manner to demonstrate compliance with its obligations and to enable verification in accordance with Article 28(3)(h).

5 Use of further (sub-)processors

22 Involving additional (sub-)processors by the processor in the performance of the basic agreement with regard to data processing shall in principle require the prior written authorization of the controller, insofar as the provision of the main service(s) with regard to the data processing is to be contractually relocated or delegated. Subcontracting relationships that are relevant in this sense do not include, for example, auxiliary services of third parties in telecommunications, shipping/transport, IT maintenance (such as manufacturer support services and the like), user services, etc., although risk-appropriate and legally compliant contractual regulations and control measures must also be ensured in this respect.

23 However, the processor shall – to the extent necessary for the performance of the basic agreement – use as sub-processors those companies that are absolutely necessary for the performance of the basic agreement. These companies are or were disclosed to the controller in the course of the commissioning and are absolutely necessary for the provision of services. In any case, the controller has the right to object to such a commissioning. In this case, it is expressly stated that the processor can then no longer provide services under the basic contract as agreed. However, the processor shall only engage sub-processors who are objectively suitable for the specific contractual activity, in particular who offer sufficient guarantees for the necessary TOMs and who commit themselves in verifiable agreements pursuant to Art. 28 (3) of the GDPR to at least guarantee the level of data protection specified in this commitment. If the sub-processor performs the agreed service outside the EU/EEA area, the processor shall ensure the admissibility of data protection.

24 The controller shall be informed in good time of any intended change (supplement or replacement) regarding the involvement of sub-processors so that the controller can raise any objections to certain additional processors before implementation.

6 Liability

25 The Processor shall be liable to the Controller in the event of a culpable breach of this undertaking solely in accordance with the statutory provisions.

7 Term of Commitment / Termination

26 This commitment shall apply in addition to the basic agreement, i.e. in any case for as long as the processor provides services relevant under data protection law to the controller. It shall terminate without the need of separate declarations upon complete cessation of the basic agreement relationship (for whatever reason) or by revocation by the processor.

8 Final Provisions

27 Amendments or supplements to this commitment, including the mutually agreed waiver of the requirement of written form, must be made in writing, whereby the transmission of electronic notifications and messages to the last e-mail contact address given is sufficient.

28 Should individual parts of this commitment be or become invalid, this shall not affect the validity of the remaining parts. An omitted provision shall be replaced by the permissible or valid provision that comes closest to the processor's obligation under the GDPR. The same procedure shall be followed in the event of regulatory gaps.

Vienna 09/01/2024
Place/Date

SIGNATURE INFORMATION	**Signatory**	Franz Semmernegg
	Date/Time-UTC	2024-01-15T12:41:48+01:00
	Verification	Information about the verification of the electronic signature can be found at: https://www.signature-verification.gv.at
Note	This document is signed with a qualified electronic signature. According to EU regulation No 910/2014 (eIDAS) it is legally equivalent to a handwritten signature.	

CANCOM	**Unterzeichner**	Mag. Christian Urban, ppa
	Datum/Zeit-UTC	2024-01-15T11:36:38+01:00
Prüfinformation	Signiert mit PrimeSign, einem Produkt der PrimeSign GmbH. Informationen zur Prüfung finden Sie unter http://www.signaturpruefung.gv.at	

Dr. Franz SEMMERNEGG
Executive Board
CANCOM Austria AG

Mag. Christian URBAN
Vice-President Legal
CANCOM Austria AG

Annex

Technical and organizational measures (Article 32 (1) GDPR)

The processor shall ensure data security and a level of protection appropriate to the processing risk and in line the technical state of the art with regard to confidentiality, integrity and availability of data as well as with regard to the resilience of systems. In order to always guarantee a level of protection in line with the current state of the art, the processor is certified in accordance with ISO 9001 and ISO 27001 and strives to maintain these certifications on an ongoing basis. In addition, the processor is qualified to carry the Cyber Trust Austria Gold Label.

It is noted that all aforementioned measures apply and have been implemented only in the processor's premises and sphere of access. The processor assumes no responsibility or liability for the technical or organisational measures necessary and/or applicable within the sphere of power and influence of the responsible party. In particular, facilities, personnel, IT infrastructure, objects and data located within the area of responsibility of the responsible party are excluded.

Insofar as relevant for the performance of the basic agreement, the following measures have already been taken (or will be taken in due time) by the processor in his system environment:

Access control (physically)

- ✓ Identity check done by doorman or security service
- ✓ Surveillance on weekends/ public holidays
- ✓ Alarm and warning devices/ burglar system
- ✓ Video monitoring of access areas
- ✓ Restricted access to office and business premises
- ✓ Safety locks
- ✓ Safeguard of building shafts, back doors, side entrances etc.
- ✓ Motion detector/photoelectric sensors
- ✓ Feedback control with chip card or transponder
- ✓ Key provisions
- ✓ Manual locking system
- ✓ Keeping record of key issuing/chip card issuing/ transponder issuing
- ✓ Issuance of master key
- ✓ Regulation of access for visitors (registration, record keeping)
- ✓ Mandatory wearing of an authorization card for Visitors
- ✓ Specific safeguarding/entry barriers of server rooms and archives

Access control (technically)

- ✓ Secure storage of data media
- ✓ „clean desk" (digital workplace, cleaning of virtual desktop)
- ✓ Securing of internal interfaces (WLAN, LAN etc.)
- ✓ Guidelines for password security
- ✓ Authorisation concept
- ✓ Creation of user profiles

- ✓ Assignment of rights and roles to data processing systems
- ✓ Authentication with unique user ID
- ✓ Two-factor authentication and MFA
- ✓ Authentication with username and password or option for biometric logon
- ✓ Secure connection for remote maintenance
- ✓ Recording of access (log-on and log-off) to data processing systems inkl. SIEM
- ✓ Account lock in case of incorrect attempt to access
- ✓ Automatically locked computer when temporary absent
- ✓ Regularly forced password change
- ✓ Immediate blocking of entitled/authorized users, who have left the company
- ✓ Administration of rights by System Administrator
- ✓ Secure storage of the administrator password
- ✓ Attack detection systems/ antivirus software and behaviour-based malware / ransomware detection as well as sandboxing for servers and workstations (SoC, EDR)
- ✓ Protection through firewall incl. intrusion detection & prevention system
- ✓ Data encryption/Hard disk encryption of mobile end devices (smartphone, notebook, USB-Stick etc.)
- ✓ Use of protection programs and administration software on smartphones and tablets
- ✓ Prohibition on the unauthorized installation of software and hardware
- ✓ Regular updating of protection programs (updates, etc.)

Access control (safety precautions)

- ✓ Access restriction for computer systems and network drives to authorized users
- ✓ Access restriction for backup disks to system administrators
- ✓ Encryption of back-ups in an isolated environment
- ✓ Authorization concept
- ✓ Process for requesting, approving, granting and returning access authorization
- ✓ Minimization of authorization according to the purpose-specification and limitation principle (the principle of least privilege)
- ✓ Differentiated authorizations
- ✓ Authorization management by System Administrator
- ✓ Reporting and analysis of an attempted/effected security breach
- ✓ Overwriting of data media with appropriate software before recycling/reuse
- ✓ Proper destruction of data media
- ✓ Use of appropriate data protection containers to prevent unauthorized removals
- ✓ Reporting/logging of data disposal
- ✓ Encryption of data media

Transmission control

- ✓ Monitoring of data communication/data traffic
- ✓ Encrypted and program-controlled transfer of data
- ✓ Cryptographic coding procedures (e.g. S/ MIME))
- ✓ Data transfer via secure connections (e.g. https/SFTP)
- ✓ Keeping record of demand processes and transmission processes
- ✓ Setup of dedicated lines or VPN solutions (SD WAN)
- ✓ Use of passwords and password security
- ✓ Separate paths for password transmission

Input control

- ✓ Traceability of accesses based on individual user names
- ✓ Traceability of accesses based on user groups
- ✓ Keeping record/logging of input, modification and deletion of data
- ✓ Authenticity (data can be assigned to its origin at any time)

- ✓ Overview of applications used to enter/modify/delete data

Order control
- ✓ Selection of further (sub-)processors, e.g. call center, according to date security guarantees
- ✓ Obligation of all processors pursuant to Article 28 (3) GDPR
- ✓ Careful selection of service providers (IT, security, cleaning, waste disposal, transport and other service providers)
- ✓ Data protection audits at the processor
- ✓ Ensuring return/proper destruction of all data at the end of the contract
- ✓ Compliance with the requirements of the GDPR for data processings in third countries
- ✓ Risk based audits of data processing in third countries

Availability control
- ✓ Data backup concept
- ✓ Maintaining backup directories or a backup directory structure
- ✓ Emergency plan/Recovery concept
- ✓ Backup data center
- ✓ Data recovery tests
- ✓ Use of specific monitoring programmes
- ✓ Uninterrupted power supply (UPS)
- ✓ Fire detections systems and smoke detections systems
- ✓ Fire extinguishers
- ✓ Special fire/water ingress protection for server rooms and archives
- ✓ Temperature monitoring/ humidity control/ air-condition in server rooms and archives
- ✓ Coordinated and implemented requirements for data availability and processability
- ✓ Minimizing the entry points for malware (disabling of dispensable services)

Principle of separation
- ✓ No shared use of office space, archives and servers by outside companies
- ✓ Separate data storage on separate systems, drives and volumes
- ✓ Logical client separation
- ✓ Specification of database rights (access barriers for individual folders, data records, fields)
- ✓ Division of roles regarding users
- ✓ Authorisation concept
- ✓ Management of authorizations by the system administrator
- ✓ By means of authorization concept separate storage of particularly sensitive data (e.g. personnel area)
- ✓ Separation of development, test and live systems
- ✓ Informational separation of powers

Organisation
- ✓ Appointment of the data protection officer
- ✓ Obligation of employees to maintain data confidentiality
- ✓ Obligation of agency staff to maintain data confidentiality
- ✓ Data protection training for employees
- ✓ Information security guidelines
- ✓ Regulation of private use of company communications technology
- ✓ Direct/Adress marketing in accordance with data protection regulations
- ✓ Use of cloud computing in accordance with data protection regulations
- ✓ Regular performance if internal audits
- ✓ Data protection guideline