Unilateral Commitment Statement

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

by

CANCOM Austria AG
Wienerbergstraße 53, 1120 Vienna

(hereinafter “processor”)

on behalf of

Controller

(hereinafter “controller”),

1 Subject matter of the obligation

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 declaration to the unilateral commitment (hereinafter referred to as the “declaration of commitment”) forms the specific legal basis for data processing in accordance with Art. 28 (3) of the GDPR, with the controller acting as the (sole) “controller” and the processor acting as the “processor”. Insofar as the term “data processing” or “processing” (of data) is used in this declaration of commitment, the definition of processing within the meaning of Art. 4 (2) of the GDPR shall be used.

2 With this declaration of commitment, the processor assures the controller and undertakes to comply with and ensure compliance with all requirements arising for the processor under Article 28 of the GDPR. In particular, the processor will fulfill the obligations set forth below and implement them accordingly in the course of the processing relationship.

2 Suitability as Processor

3 The processor constitutes a processor within the meaning of Article 28(1) of the GDPR, offering sufficient guarantees that appropriate technical and organizational measures (hereinafter referred to as “TOMs”) are implemented and ensured accordingly. The TOMs implemented and guaranteed by the processor are listed in **Annex 1** to this declaration of commitment.

4 The processor warrants and undertakes that these TOMs are ensured for all data processing operations that the processor carries out on behalf of the controller. However, this applies only to the extent that the systems and accesses affected thereby are 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 purpose and means of data processing arise from the main performance obligations of the underlying Basic Agreement. 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 must be processed within the territorial scope of the GDPR unless both written authorization from the controller for a transfer to third countries and the specific requirements of Articles 44 et seq. of the GDPR are met.

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 th econtroller. 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 instructions of the controller pursuant to Article 4(7) of the GDPR and to pursue exclusively those means and purposes specified by the controller in the underlying Basic Agreement.

15 Concrete obligations or detailed behavioral guidelines that do not arise directly from the Basic Agreement or from objective law must be documented and established by the controller as “data processing instructions.”

16 The data processor warrants that all persons employed or authorized to process the data are appropriately qualified and have been bound to confidentiality (e.g., in accordance with § 6 of the Federal Act concerning the Protection of Personal Data (DSG) or § 11 of the Federal Act Against Unfair Competition (UWG)) or are subject to an appropriate – in particular statutory – duty of confidentiality (Art. 28 (3) (b) GDPR). The duty of confidentiality shall continue to be observed even after the termination of the Basic Agreement.

17 The processor expressly declares that all relevant employees have been demonstrably bound to data secrecy and confidentiality. In addition, employees receive regular training and awareness-raising on the topics of data protection and information security.

18 The processor undertakes to take all measures necessary to ensure the security of data processing in accordance with Art. 32 of the GDPR (Art. 28(3) (c) of the GDPR). In particular, the processor has taken all organizational and technical precautions 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 **Appendix 1** and comply with the security policy in accordance with ISO 27001. The certificate can be presented to the controller upon request. The processor will regularly monitor and document the effectiveness of its processes and measures and, where necessary, make or arrange for modifications in response to technical advancements.

19 The processor shall support the controller in fulfilling its information obligations and asserting the rights of data subjects to the greatest extent possible (Art. 28 (3) (e) GDPR). In particular, the processor shall create the technical and organizational conditions

necessary for the controller to meet its obligations to data subjects under Art. 15 et seq. of the GDPR (provision of information, rectification, erasure/right to be forgotten, data portability, objection) within the relevant deadlines. The processor shall in any case provide the controller with the information that can be obtained with reasonable technical and economic effort.

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

21 The processor shall inform the controller (or the controller's designated data protection officer) of any relevant breaches of the protection or security of data subject to the contract within its area of responsibility without undue delay after becoming aware of the relevant event. In particular, the following must be specified: the affected data records/data categories and individuals, the expected consequences of the data breach, the countermeasures taken or planned, and the contact details of a responsible person or other point of contact at the processor for further information or coordination.

22 The processor shall provide the controller with information in an appropriate manner to demonstrate compliance with its obligations and shall enable an audit within the meaning of Article 28(3)(h) of the GDPR.

23 The processor is not responsible for ensuring that the data, documents, and information processed for the use of the solution are complete, correct, lawful, or in a form suitable for processing. This includes, in particular, personal data as well as internal or confidential documents that are automatically evaluated, searched, or processed by a solution. The same applies to the setup and maintenance of authorizations, roles, access rights, filter rules, and other settings, insofar as these do not fall within the scope of the processor. The processor is not obligated to review the data provided by the controller in terms of content, legality, or technical aspects; no verification of accuracy, completeness, timeliness, or compliance with legal requirements takes place.

5 Use of Additional (Sub)Processors

24 The involvement of sub-processors by the processor in fulfilling the Basic Agreement with regard to data processing generally requires the written consent of the controller if the provision of the main service(s) with regard to data processing itself is to be outsourced or delegated. Sub contracting relationships are therefore not considered relevant in this sense, e.g. auxiliary services provided by third parties in the areas of telecommunications,

shipping/transport, IT maintenance (such as manufacturer support services and the like), user services, etc., although care must be taken to ensure that the contractual provisions and control measures are risk-appropriate and legally compliant.

25 For the companies listed in **Annex 2**, consent to subcontracting is deemed to have been granted provided that they are objectively suitable for the specific contractual activity, in particular that they offer sufficient guarantees for the necessary technical and organizational measures, and commit, in verifiable agreements concluded in accordance with Art. 28(3) GDPR, to at least ensuring the level of data protection specified in the present contract. If the sub-processor provides the agreed service outside the EU or the EEA, the processor shall ensure compliance with data protection law. In any case, the controller has the right to object to such an engagement. In this case, it is expressly stated that the processor will then no longer be able to provide its services under the Basic Agreements as agreed.

26 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

27 The processor shall be liable to the controller and to third parties exclusively for damages resulting from a breach of the obligations expressly imposed on it by the GDPR or by this agreement due to intentional or grossly negligent conduct. Liability for slight negligence is excluded.

28 To the extent that the controller breaches its obligations to cooperate, provide resources, or ensure quality in connection with data processing, the controller shall be liable for all damages resulting from such a breach.

29 If the processor is held directly liable by a third party or a data subject within the meaning of data protection regulations, the controller shall indemnify the processor against all damages

a) that are not based on an intentional or grossly negligent breach of duty by the processor.

b) resulting from a breach of the controller's obligations to cooperate, provide resources, or ensure quality.

7 Data Protection Officer / Representative

30 Although the legal requirements for the appointment of a data protection officer in accordance with Art. 37 GDPR are not met, the processor has voluntarily appointed a data protection officer. This serves to ensure a high standard of data protection and the best possible support for data protection concerns. The data protection officer can be reached at the email address datenschutz@cancom.com for data protection inquiries.

8 Term of the Agreement/Termination

31 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.

9 Final Provisions

32 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.

33 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, 16.04.2026
Place, Date

CANCOM	Unterzeichner	Bernd Eder
	Datum/Zeit-UTC	2026-04-16T14:18:07+02:00
Prüfinformation	Signiert mit PrimeSign, einem Produkt der PrimeSign GmbH. Informationen zur Prüfung finden Sie unter http://www.signaturpruefung.gv.at	

SIGNATURINFORMATIONEN	Unterzeichner	Christian Urban
	Datum/Zeit-UTC	2026-04-16T12:31:21+02:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument ist gemäß EU Verordnung Nr. 910/2014 (eIDAS) einem handschriftlich unterzeichneten Dokument grundsätzlich rechtlich gleichgestellt.	

Mag. (FH) Bernd Eder
Executive Board
CANCOM Austria AG

Mag. Christian URBAN
Vice-President Legal
CANCOM Austria AG

Appendix 1

Technical and organizational measures (Art. 32(1) GDPR)

The processor must ensure data security and a level of protection appropriate to the processing risk and in line with the state of the art with regard to the confidentiality, integrity, and availability of the data, as well as the resilience of systems. To ensure a level of protection in line with the current state of the art at all times, the processor is certified to ISO 9001 and ISO 27001 and strives to maintain these certifications on an ongoing basis. In addition, the processor is qualified to hold the Cyber Trust Austria Gold Label.
It is noted that all measures mentioned apply and have been implemented solely within the processor's premises and sphere of access. The processor assumes no responsibility or liability for the technical or organizational measures necessary and/or applicable within the control and influence of the controller. Specifically excluded are facilities, personnel, IT infrastructure, objects, and data within the controller's area of responsibility.

To the extent relevant for the performance of the contract, the following measures have already been (or will be implemented in a timely manner) by the data processor in its system environment:

Access control (physically)

- ✓ Personnel checks by a doorman or security/guard service
- ✓ Security on weekends and holidays
- ✓ Physical security plan
- ✓ Alarm system/burglar alarm system
- ✓ Video surveillance of entrances
- ✓ Access restrictions for office and business premises
- ✓ Security locks
- ✓ Securing building shafts, back doors, side entrances, etc.
- ✓ Smart card/transponder system
- ✓ Key management
- ✓ Manual locking system
- ✓ Logging of key/smart card/transponder issuance
- ✓ Master key system
- ✓ Visitor access control (registration, logging)
- ✓ Requirement to wear visitor ID badges
- ✓ Special security measures/access restrictions for server rooms and archives

Access control (technically)

- ✓ Secure storage of data storage media
- ✓ “Clean desk” (digital workspace, cleaning of the virtual desktop)
- ✓ Securing internal interfaces (Wi-Fi, LAN, etc.)
- ✓ Password security policy
- ✓ Authorization concept
    - Creation of user profiles
    - Assignment of rights and roles to data processing systems
- ✓ Authentication via unique user ID
- ✓ Two-factor authentication and MFA
- ✓ Authentication via username and password or the option for biometric login
- ✓ Secure connection for remote maintenance
- ✓ Logging of access (login and logout) to data processing systems, including SIEM
- ✓ Account lockout upon failed login attempts
- ✓ Automatic computer lockout during temporary absence
- ✓ Regular mandatory password changes
- ✓ Revocation of access rights for former users
- ✓ Management of permissions by the system administrator
- ✓ Secure storage of the administrator password
- ✓ Intrusion detection system/antivirus software, as well as behavior-based malware/ransomware detection and sandboxing for servers and workstations (SoC, EDR)
- ✓ Firewall isolation, including intrusion detection and prevention systems
- ✓ Data/hard drive encryption for mobile devices (smartphones, laptops, etc.)
- ✓ Use of security programs and administration software on smartphones and tablet PCs
- ✓ Prohibition of unauthorized installation of software and hardware
- ✓ Regular updating of security programs (updates, etc.)

Access control (safety precautions)

- ✓ Restriction of access to computer systems and network drives to authorized users
- ✓ Restriction of access to backup media to system administrators
- ✓ Encryption of backups in an isolated environment
- ✓ Authorization Policy
- ✓ Process for requesting, approving, granting, and revoking access permissions
- ✓ Minimization of permissions according to the principle of least privilege
- ✓ Authorization management by the system administrator
- ✓ Reporting and analysis of actual or attempted security breaches
- ✓ Overwriting of data storage media with appropriate software prior to reuse
- ✓ Proper destruction of data storage media
- ✓ Use of appropriate data protection containers to prevent unauthorized removal
- ✓ Logging of data disposal

Transmission control

- ✓ Monitoring of data traffic
- ✓ Encrypted, program-controlled transmission of data
- ✓ Cryptographic encryption methods (e.g., S/MIME)
- ✓ Data transfer via secure connections (e.g., HTTPS/SFTP)
- ✓ Logging of retrieval and transmission processes
- ✓ Setup of dedicated lines or VPN procedures (SD-WAN)
- ✓ Use of passwords and password security
- ✓ Separate channels for password transmission

Input control

- ✓ Traceability of access based on individual usernames
- ✓ Traceability of access based on user groups
- ✓ Logging of data entry, modification, and deletion
- ✓ Authenticity (ability to trace data back to its source at any time)
- ✓ Overview of the applications used to enter, modify, or delete data

Order control

- ✓ Selection of additional (sub)processors, e.g., call centers, based on data security guarantees
- ✓ Obligations of all processors pursuant to Article 28(3) of the GDPR
- ✓ Careful selection of IT, security, cleaning, waste disposal, transportation, and other service providers
- ✓ Data protection audits at the data processor
- ✓ Ensuring the return or proper destruction of all data upon termination of the contract
- ✓ Compliance with the requirements of the GDPR for data processing in third countries
- ✓ Risk-based assessments of data processing in third countries

Availability control

- ✓ Data backup strategy
- ✓ Maintenance of backup directories or a backup directory structure
- ✓ Contingency plan/recovery concept
- ✓ Backup data center
- ✓ Data recovery tests
- ✓ Use of specialized monitoring programs to monitor availability
- ✓ Uninterruptible power supply (UPS)
- ✓ Fire and smoke detection systems
- ✓ Fire extinguishers
- ✓ Special fire/water ingress protection for server rooms and archives
- ✓ Temperature/humidity monitoring and air conditioning in server rooms and archives
- ✓ Coordinated and implemented requirements for data availability and processability
- ✓ Minimization of entry points for malware (shutdown of non-essential services)

Principle of separation

- ✓ No shared use of office spaces, archives, and servers by third-party companies
- ✓ Physically separated data storage on separate systems, drives, and storage media
- ✓ Logical client separation
- ✓ Definition of database permissions (access restrictions for individual folders, records, and fields)
- ✓ Role separation of users
- ✓ Authorization concept
- ✓ Separate storage of particularly sensitive data (e.g., HR data) using an authorization concept
- ✓ Separation of development, test, and production systems
- ✓ Separation of informational powers

Organization

- ✓ Appointment of a data protection officer
- ✓ Appointment of an information security officer
- ✓ Obligation of employees to maintain data confidentiality
- ✓ Obligation of external personnel to maintain data confidentiality
- ✓ Data protection training for employees
- ✓ Information security policies
- ✓ Regulations on the private use of company communication technology
- ✓ Direct/address marketing in accordance with data protection regulations
- ✓ Use of cloud computing in accordance with data protection regulations
- ✓ Regular internal audits
- ✓ Data Protection Policy

Appendix 2

List of Sub-Processors Used

The controller has approved the use of the following Sub-Processors:

1. Sub-Processor

Name:	CANCOM GmbH
Address:	Erika-Mann-Straße 69, 80636 Munich
Description of processing:	Provision of the ServiceNow platform for IT service management; IT services.
Location of data processing:	EU

a. Sub-Subprocessor

Name:	ServiceNow B.V.
Address:	Hoekenrode 3, 1102 BR Amsterdam, Netherlands
Description of processing:	Provision of the ServiceNow platform for IT service management.
Location of data processing:	EU

b. Sub-Subprocessor

Name:	ONEIO Cloud OY
Address:	Huopalahdentie 24, FL-00350 Helsinki, Finland
Description of processing:	Technical interface between Cancom Service Now and customer ITSM systems for ticket information without temporary storage of data.
Location of data processing:	EU

c. Sub-Subprocessor

Name:	SOLVVision AG
Address:	Rheinstraße 29, 60325 Frankfurt am Main
Description of processing:	System implementation
Location of data processing:	EU

d. Sub-Subprocessor

Name:	agineo GmbH
Address:	Pascalstraße 25, 52076 Aachen
Description of processing:	System implementation
Location of data processing:	EU

2. Sub-Processor

Name:	CANCOM Converged Services GmbH
Address:	Wolfganggasse 58-60, 1120 Vienna
Description of processing:	Use of ServiceNow for the provision of IT services to customers, as well as the implementation, maintenance, and operation of IT systems.
Location of data processing:	EU

3. Sub-Processor

Name:	Atlassian Pty Ltd.
Address:	George Street, Sydney, NSW 2000
Description of processing:	Use of cloud services provided by Atlassian for project management, knowledge documentation, and the administration, assignment, and processing of tasks.
Location of data processing:	Headquarters in Australia, data hosted in the EU

4. Sub-Processor

Name:	Microsoft Azure
Address:	Microsoft Corporation, One Microsoft Way Redmond, WA 98052-6399, USA
Description of processing:	Provision of cloud infrastructure.
Location of data processing:	Headquarters in the US, data hosted in the EU

5. Sub-Processor

Name:	Hays Austria GmbH
Address:	Europaplatz 3/5, 1150 Vienna
Description of processing:	Recruitment of external personnel for the provision of IT services.
Location of data processing:	EU

6. *Sub-Processor*

Name:	CANCOM a + d IT solutions GmbH
Address:	Heinrich Bablik-Straße 17/K21, 2345 Brunn am Gebirge
Description of processing	Provision of smart workplace solutions.
Location of data processing:	EU