**Contract**

**on Processing of Personal Data on Behalf of a Controller**

between

Crnogorski Telekom a.d.

Ulica Moskovska br. 29, Podgorica, Crna Gora

PIB 02289377, PDV 20/31-00049-4

– hereinafter referred to as the "Controller" –

and

– hereinafter referred to as the "Processor" –

– hereinafter referred to individually and collectively as the "Party"/"Parties" –

**§ 1 Subject matter of the Contract; legal basis**

(1) This Contract (hereinafter referred to as "Framework CDP") governs the processing of personal data (hereinafter referred to as "Data") by the Processor for and on behalf of the Controller, according to the Controller's instructions, in connection with (add name of Main Agrrement)executed by the Parties on <…> (hereinafter referred to as the "Main Agreement").

(2) This Framework CDP applies to all future orders and any already placed orders under the Framework Agreement.

(3) In the event that the Controller processes the personal data covered by this Contract on behalf of a Superordinate Customer, i.e., if the Data to be processed is personal data of a client of the Controller, the Processor shall also, on request of the Controller, extend the granting of information and monitoring rights to include this Superordinate Customer or client (hereinafter referred to as "Superordinate Customer") in accordance with § 2 (4), § 3 (5-8), and § 6, or to a lesser extent as defined by the Controller. In this case the Processor shall continually provide the Controller with details on the information given and checks carried out in writing or by e-mail

(4) This Contract is based on the provisions of the applicable laws of the European Union (in particular the EU General Data Protection Regulation) and of the Member States (referred to jointly as "Legal Provisions"),as well as applicable laws of Montenegro.

**§ 2** **Provision of Data; Services, purpose and location of the Processing Rights and obligations of the Controller**

(1) **[Provision of Data]** The Controller shall provide the Processor with access to the Controller's Data as described bellow

 1. Data to be processed/Data affected; type of access;

The Controller commissions the data processing under the following terms and conditions:

a. Categories of data subjects:

• Enduser of the Controller

• Employees of the Controller

(Please choose one or boht categories of data subject)

b. Affected personal data:

• Last name/first name

• Company name

• Contact data (e.g., telephone, e-mail)

• Traffic data (data that is collected, processed, or used during the provision of a telecommunications service, e.g., the telecommunications service used, the number or the ID of the lines involved (calling party and called party), the card number (if customer cards are used), any location data for cell phones, the be-ginning and end of the individual call (date and time), and the data volumes transmitted).

• Customer and End Customer Data of the ControllerCharging records

• User names

• IP address

• MSISDN of enduser of the Controller

• IMSI of enduser of the Controller

• IMEI

 Message Content of enduser of the Controller

• Location Data

• Cell ID

• Location Area (LAC)

• Mobile Country Code (MCC)

• Mobile Network Code (MNC)

• Account and log in data of

• Users of telecommunications services

• Subscribers

(please choose affected pesonal data from the list or add personal data)

Given the nature of the Services, the Controller verifies that the Processor is unable to confirm or maintain the list of affected Personal Data listed above. Therefore, the Controller will notify the Processor of any changes necessary to the above-mentioned list in writing. The Processor will process all categories of Personal Data of the Controller listed above in accordance with the Agreement. If changes to the Controller’s Personal Data Lists require changes to the agreed processing, the Controller will provide Processor with Additional Instructions as specified in the Agreement.

c. Sensitive Data/Special categories of Data within the meaning of Art. 9 of the EU General Data Protection Regulation (GDPR) (must be specified in detail here):

• (please add sensitive data or n/a)

d. Access to personal data

1 Services in the area of maintenance, remote maintenance and/or IT fault analysis shall be provided. The possibility that the Processor may get access to the Data cannot be excluded in the context of performance of these services.

Access provide via:

• In accordance with the regulations for remote access via a CRD portal as agreed between the Parties. The Controller is responsible for the adequate security level of the CRD portal. With respect to this, the Processor is not responsible to imply any technical and organizational measures that are marked with “This requirement is met by use of a CRD-portal…” in the Annex 1 of this agreement.

• In individual cases in form of Files, which are transmitted over Secure File Transfer System (Secure FTS of the CRD-Portal) to the Processor. These data may only be processed by the necessary employees and must be deleted without undue delay after the end of the individual case. Because this data will be stored outside the CRD-Portal and the Systems of the Telekom, the Processor must implement the corresponding TOM marked in Annex1 himself.

• On-site

(please choose relevant access tipe)

2. Services, purpose and location of the Processing:

Any related processing of data will be done for the purpose of (please describe the servis from the Main agreement)

The Processor may provide the services mainly from Montenegro but (also) from the countries of the European Union, the European Economic Area or in third countries, using approved subcontractors as listed in Annex 2, in accordance with Frame CDP.

(2) **[Responsibility]** In relation to the Processor, the Controller is solely responsible for assessing whether Data can be processed lawfully and for safeguarding the rights of the data subjects.

(3) **[Instructions**] The Controller has the right to issue instructions on the type, scope, and methods of data processing. All instructions shall be issued in writing or by e-mail. Unless otherwise necessary to comply with applicable data privacy law, any changes or additions to the instructions must be agreed to according to the process for amending the Agreement.

(4) [Audits] The Controller may check the Processor's compliance with the Legal Provisions and this Contract(for regular audits Controller will notify audits 30 days in advance) at any time and without undue delay at Controller’s own costs and expense unless such audits show non-compliance with data privacy as agreed even at the Processor's premises, in particular by obtaining information and viewing the stored Data and the data processing programs on the Processor's premises. In the case of maintenance/remote maintenance, the Parties may conclude further necessary agreements, as appropriate. The Controller may perform the checks itself or have them performed by a contracted independent, qualified third party who is obligated to maintain confidentiality. If the Purchaser decides to appoint a third-party auditor, it must indicate the name and the firm of the auditor. Supplier has the right to refuse the appointment of a third-party auditor to the extent for good cause. The audit may not be conducted by any competitor of the Supplier.

The Controller shall announce checks to be carried out at the Processor within a reasonable period of time, perform the checks during normal business hours only, and take due care during their performance not to disturb the Processor's business operations and operational workflows; however, this does not apply in the case of a specific suspicion of abuse. The methodology of the audit has to be shared with Supplier and it must be designed to minimize disruption to Supplier’s operations. The Purchaser has to indicate the schedule, the accurate scope of the audit as well as the identity of the person(s) in charge of performing the audit.

(5) **[Right to proof]** The Controller has the right to request proof from the Processor with regard to the fulfillment of the Processor's obligations.

**§ 3** **Rights and obligations of the Processor**

(1) **[Purpose of processing**] The Processor shall provide the Controller with the services/process the Data for the purposes described in the Framework CDP.

(2) **[Lawfulness of processing**] The Processor shall process the Data in accordance with the Legal Provisions, the provisions of this Contract, and the instructions of the Controller. If, due to a Legal Provision, the Processor is prevented from processing the Data in accordance with this Contract and the instructions of the Controller, it shall inform the Controller of this before carrying out the processing, unless it is legally forbidden under Union or Member State Law to inform the Controller on important public interest grounds. The Processor shall not use the Data for any other purpose and shall in particular not be permitted to pass on the Data provided to it to third parties. Copies and duplicates must not be created without the prior consent of the Controller. This excludes backups required to assure proper data processing.

 In the case of maintenance, remote maintenance and/or IT fault analysis, access to the Data of the Controller shall be prevented as far as possible. If Data access is unavoidable, the Processor must limit Data access to the unavoidable minimum.

(3) **[Data protection officer]** The Processor provides assurance that it has engaged a competent and reliable data protection officer, who is granted the time required to perform his or her duties. The data protection officer performs the duties in accordance with the Legal Provisions; in particular, he/she takes steps to ensure compliance with the legal and agreed regulations regarding data protection.

As far as the engagement of a data protection officer is not required by law and the Processor therefore does not have a data protection officer in place the Processor determines a contact person responsible for the matter of data protection.

Detailed information on the contact details of the data protection officer / the responsible contact person is provided in § 8 below.

(4) **[Territorial restrictions**] The data processing may generally take place in a Member State of the European Union/European Economic Area. The location of processing is (add the location). Changes regarding the processing location and/or the inclusion of further processing locations require the prior agreement of the Controller (in writing or by e-mail).

Data processing in third countries (i.e. countries that are not member states of the European Union/European Economic Area and do not possess an accepted appropriate level of data protection) shall only take place on the basis of an additional, separate agreement (EU Standard Contractual Clauses) to ensure an appropriate level of data protection. Furthermore Processor agrees to enter into separate EU Standard Contractual Clauses directly with a respective Superordinate Customer (Data Exporter), as defined in § 1 (3), if necessary. Processor is obligated to enter into the EU-Standard Contractual Clauses in the name and on behalf of Controller and/or, if so, the respective Superordinate Customers with its Subprocessors in third countries which are approved by Controller. The power of attorney for this purpose is hereby granted by the Controller. Controller is obligated to obtain a respective power of attorney from its Superordinate Customers. If Processor offers safeguards according to Article 46 GDPR to Controller, it is in Controller´s discretion to decide, if processing in third countries can be carried out on that basis. § 6 remains unaffected.

The foregoing provisions also apply to any access to or viewing of the Data by the Processor, e.g., as part of internal checks or for the purpose of development, carrying out tests, or administration.

(5) **[Audits]** With regard to § 2 (4) above, the Processor shall provide information and cooperate accordingly. The Processor shall support the Controller in particular in data protection audits conducted by the supervisory authorities to the extent that such audits concern the processing of Data under this Contract, and shall immediately implement the requirements of the supervisory authority in agreement with the Controller.

The Processor itself must also monitor compliance with the Legal Provisions and this Contract. Checks must be carried out by the Processor at regular intervals to review the effectiveness and success of the technical and organizational data protection measures implemented. Evidence of the implementation of contractually agreed measures must, upon request of the Controller, be presented in the form of up-to-date attestations, reports, or extracts thereof.

(6) **[Data subjects exercising their rights]** On the instructions of the Controller, the Processor is obliged to support the Controller in fulfilling its obligations toward data subjects who are exercising their rights in accordance with the Legal Provisions (e.g., right to information, correction).

 If a data subject addresses the Processor directly, the Processor shall not disclose any information, but rather refer the data subject to the Controller. The Processor shall inform the Controller accordingly.

(7) **[Further support]** The Processor shall also support the Controller in the performance of its other legal duties where these are associated with the data processing by the Processor. In particular, it shall:

(a) on request, provide the Controller with all the information it has at its disposal that the Controller needs to comply with its reporting and/or documentation duties in accordance with the Legal Provisions (in particular the records of processing activities);

(b) support the Controller in providing information to the extent that information about the processing of Data is required to be reported to a governmental agency or a person in accordance with the Legal Provisions;

(c) inform the Controller of any incidents of serious disruption to operations, any suspicion of data protection violations, and/or other irregularities in relation to the processing of the Data. The Processor is aware that the Controller is obliged to inform the supervisory authorities immediately of any data protection violations. The relevant information shall be documented and shall contain the details necessary for reporting to the supervisory authorities. In the event of data protection violations, the Processor shall support the Controller in notifying the data subjects and the supervisory authority, if requested to do so.

(8) The Processor shall immediately notify the Controller of any and all communications from the supervisory authorities (e.g., inquiries, notification of measures or requirements) to the Processor in connection with the processing of Data under this Contract. Subject to mandatory statutory requirements under Union or Member State Law, the Processor shall only provide information to third parties, including supervisory authorities, with the prior consent of and in consultation with the Controller (in writing or by e-mail).

(9) **[Deletion or return of data]** Upon completion of the commissioned work or earlier at the request of the Controller, the Processor shall delete all personal data or destroy data carriers containing personal data in accordance with current and recognized technical standards in such a way that recovery of the Data is not possible or only possible with disproportionate effort, and shall confirm this to the Controller stating the methodology used. The destruction of data carriers shall be recorded stating the serial number of the data carrier, and the type and date of destruction. The aforesaid shall also apply to test and waste material and any backup copies produced.

Instead of deletion/destruction – and if agreed – the Processor shall hand over to the Controller the Data and any documents, processing results, and data carriers in its possession.

Deviations from the above deletion and return obligations shall only be considered if the Legal Provisions stipulate the storage of the personal data. The Processor shall inform the Controller of this.

**§ 4** **Technical and organizational security measures**

1. The Processor shall ensure that the Controller's Data is processed exclusively in compliance with the technical and organizational measures required in accordance with the Legal Provisions and this Contract. The measures currently required are described in **Annex 1**.
2. Any substantial security-related decisions on the organization of data processing and the applied procedures must be agreed with the Controller.
3. With regard to data processing systems owned by the Controller to which the Processor gets access, the Controller reserves the right to perform quality assurance audits and to take measures to identify misuse of such systems (e.g. Logs). This may include accessing the personal data (such as but not limited to individual user IDs and names, contact information, etc.) of those employees of the Processor who have access to the systems. The Processor has to provide via internal measures, which may also involve the participation of employee representatives, that the Controller is legally authorized to use this data.

(4) Where services in the area of maintenance, remote maintenance and/or IT fault analysis are provided, the following regulations shall also apply:

(a) The Processor's employees must use appropriate identification and encryption procedures. Before the work is performed, the Controller and Processor shall agree on any necessary Data backup measures.

(b) All services shall be documented and logged by the Processor.

(c) The Data may only be used if this has been explicitly requested by the Controller and only for fault analysis purposes. The Data may only be used on the equipment provided by the Controller or on the Processor's equipment that has been approved by the Controller for this purpose beforehand. The Data may not be copied to mobile storage media (PDAs, USB flash drives, or similar devices) without the Controller's explicit consent.

**§ 5 Confidentiality**

1. The Processor shall ensure that only persons who have first been bound by confidentiality or are subject to an appropriate legal obligation to secrecy are authorized to process the personal data. It shall ensure that personal data is not processed without authorization, in particular for other purposes, and that it is not disclosed to third parties. The Processor shall ensure that persons entrusted with the data processing are familiarized with the specifications and instructions in this Contract in advance.
2. If, in the scope of its activities, it is possible for the Processor to access electronic communications data, it shall ensure that the confidentiality obligation on the persons entrusted with the processing extends to the content and precise circumstances of the electronic communication of the data subject, in particular the involvement of the data subject in an electronic communication process and the precise circumstances of failed communication attempts.
3. The Processor guarantees that the obligation for confidentiality continues even after the end of this Agreement, after the termination of this contract and after the end of the employment or assignment relationship of the persons entrusted with the processing. If all privacy relevant Data is finally deleted or anonymized after contract cancelation, this required is also fulfilled.

**§ 6** **Subprocessors**

(1) **[Authority]** The Processor may employ other Processors ("Subprocessors"), which are listed in the Anex 2 . Additional/other Subprocessors may be employed on the condition that the Processor informs the Controller in writing or by e-mail of any intended order and/or change in respect of the inclusion or change of a Subprocessor. It may proceed as suggested if the Controller raises no objection within 10 calendar days from receipt of the information, or within a different period agreed by the Parties. It is clarified that Subprocessors may only be employed within the scope of the agreements of the Individual CDP. No subcontracting relationships within the meaning of this provision are those contracts on the basis of which the Processor – according to a mutual understanding with the Controller – merely makes use of ancillary services and these services do not include the processing of Data for the Controller (e.g., cleaning staff).

(2) **[Back-to-back agreement]** The Processor ensures that the Subprocessor is obligated toward the Processor in the same manner that the Processor is obligated toward the Controller under this Contract.

The Processor must check compliance with the obligations on the part of the Subprocessor, in particular compliance with the agreed technical and organizational measures, before data processing begins and at regular intervals thereafter. The results of these checks shall be documented and made available to the Controller upon request. Any substitution of such checks on the basis of an approved code of conduct or an approved certification mechanism with regard to the Subprocessor requires the prior consent (in writing or by e-mail) of the Controller.

(3) **[Controller's direct monitoring rights**]

The Processor also ensures that the Controller has the same monitoring rights over the Subprocessor that the Controller has over the Processor itself, and the Processor must safeguard this contractually. In the case of § 1 (3), the Processor shall ensure that the Superordinate Customer has the same rights as the Controller.

The Processor has to provide the Controller with information on the content of the contract with the Subprocessor that is essential for the monitoring rights and on the implementation of data protection-relevant obligations on the part of the Subprocessor when requested to do so.

1. **[Confidentiality]** The Processor is permitted to pass on Data to the Subprocessor or to start services in the area of maintenance/remote maintenance/IT fault analysis only if the Subprocessor has obligated its employees to observe confidentiality pursuant to § 5 of this Contract and it has implemented the agreed technical and organizational security measures.

(5) **[Sub-Subprocessor]** The Processor may permit the employment of Sub-Subprocessors (i.e., contractors of the Subprocessor; also "2nd subcontracting level”), which are listed in the Annex 2. The employment of additional/other Sub-Subcontractors (2nd subcontracting level) is only permissible with the prior agreement of the Controller (in writing or by e-mail). It is hereby clarified that Sub-Subprocessors may only be employed within the scope of the agreements.

The use of further subordinate Subprocessors (also referred to as "3rd subcontracting level) is not permitted. The Processor shall contractually forbid its Subprocessors (2nd subcontracting level) from using further Subprocessors (3rd subcontracting level).

With regard to the commissioning of Sub-Subprocessors (2nd subcontracting level), the regulations according to § 6 (2), (3), and (4) apply accordingly, especially the direct monitoring rights of the Controller vis-à-vis the Sub-Subprocessor. The Processor has to ensure that its Subprocessors impose the same obligations on their Sub-Subprocessors as are imposed on the Subprocessor vis-á-vis the Processor – but with an additional clause that excludes the use of any further Subprocessors. The Subprocessor that has employed the Sub-Subprocessor must be displayed to the person responsible.

(6) **[Overview]** The Processor shall maintain an up to date overview of the Subprocessors and Sub-Subprocessors employed and make this available to the Controller on request.

**§ 7** **Term and termination of the Contract**

(1) This Contract shall be valid for as long as the Framework Agreement, remains in force, depending on whichever remains in force for longer.

1. The Controller may, at its discretion, terminate this Framework Agreement with the Processor at any time without notice, if the Processor is in serious breach of this Contract, e.g. but not limited to, if the Processor fails to carry out instructions in accordance with § 2 (3), or if the Processor refuses to allow inspections by the Controller, whether in whole or in part, in breach of the Contract.

**§ 8** **Contacts:**

(1) The Processor's contact is:

Data protection officer:

E-mail:

(2) The Controller's contact is:

Contact:

 Title:

Telephone:

 E-mail:

(3) The Controller's data protection officer is:

Contact: Dana Bogetic Lakovic

Title: Data Privacy Officer

E-mail: dana.bogeticlakovic@telekom.me

 Data.protection@telekom.me

**§ 9 Liability; penalty**

1. The Processor's liability toward the Controller with regard to culpable breaches of this Contract shall be based on the statutory provisions. Limitations of liability agreed in this Framework Agreement shall not apply to violations against this Framework Agreement.
2. The Processor shall indemnify the Controller against such third-party claims that are filed against the Controller and are attributable to a data breach as defined in the GDPR caused by Processor by violating against the obligation under this Agreement.
3. The Processor is liable for any fault on the part of its Subprocessor and Sub-Subprocessors as if the Processor itself were at fault.
4. The Processor bears the burden of proof that any damage or any loss suffered was not the consequence of a circumstance for which it is responsible, to the extent that Data is processed under this Contract. The Processor meets its obligation to provide proof if it is able to disclose that it has observed the provisions of this Contract when collecting or processing the Data and, in particular, that it has implemented the technical and organizational measures as agreed.

**§ 10** **Miscellaneous**

(1) **[No right of retention]** The Processor shall not retain any of the Data for the reason that the Processor itself has a right of any kind against the Controller.

(2) **[Secure Data]** If Data is jeopardized on the Processor's premises due to actions by Third Parties, such as seizure or confiscation, through insolvency or settlement proceedings or by other events, the Processor must notify the Controller accordingly without undue delay and inform such Third Parties, that the Controller is the owner of the Data. The Processor shall copy the Data to secure data carriers and erase the jeopardized data in compliance with data protection laws and the relevant current and recognized technical standards.

(3) **[Validity of Contract]** The invalidity of a provision of this Contract shall not affect the validity of the remaining provisions. If a provision proves to be invalid, the Parties shall replace it with a new provision which approximates the intentions of the Parties as closely as possible.

(4) **[Changes to the Contract]** Any changes to this Contract or to an Individual CDP and any side agreements shall be made in writing (including by e-mail). This shall also apply to the waiver of this written form clause itself.

1. **[General Terms and Conditions]** The Parties agree that the "General Terms and Conditions" of the Processor shall not apply to this Contract.
2. [**Place of jurisdiction]** The sole place of jurisdiction for any disputes arising from and in connection with this Contract shall be Podgorica,Montenegro.
3. **[Applicable law]** This Contract is subject to the Legal Provisions as stipulated above in § 1 (4).

**Annex:**

The following Annexes are integral parts of this Contract:

Annex 1: Technical and organizational measures

Annex 2: List of subprocessors

|  |  |
| --- | --- |
| Controller:Crnogorski Telekom ADPlace, date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Processor:Place Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Annex 1**

**Technical and organizational security measures**

[ ] Case variant 1:

The Processor uses his own (or a subprocessor's) IT infrastructure (server/client, application) or his own end devices, either exclusively or in addition. Or:

The Processor or a Subprocessor stores personal data of the Controller in his own IT infrastructure or in his own end devices.

The following measures apply:



**OR:**

[ ] Case variant 2:

The Processor uses the Controller's IT infrastructure (server/client, application) and uses his own (or a Subprocessor's) end devices to access it. No data is stored by the Processor or a third party.

The following measures apply:



**OR:**

[ ] Case variant 3:

The Processor uses only the IT infrastructure (server/client, application) and end devices of the Controller.

The following measures apply:



**Annex 2**

**List of Subprocessors**

The following Subprocessors may be deployed for the following services:

Subprocessor:

Data protection officer:

Services:

Processing location (address):