Medloop Ltd.
24 Old Queen Street,
London, SW1H 9HP

Data Processing Agreement

between

[.....]
[.....]

hereinafter referred to as the "**Controller**"

and

Medloop Ltd
24 Old Queen Street, London, SW1H 9HP

hereinafter referred to as the "**Processor**"

Preamble

The Controller has selected the Processor to act as a service provider in accordance with Article 28 of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation, "**EU GDPR**"); and Article 28 as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc)(EU Exit) Regulations 2019 which forms the "**UK GDPR**".

This Data Processing Agreement, including all Annexes (hereinafter referred to collectively as the "**Agreement**"), specifies the data protection obligations of the parties from the underlying Principal Agreement, the Service Level Agreement and/or the order descriptions (hereinafter referred to collectively as the "**Principal Agreement**"). If reference is made to the sections of the UK Data Protection Act (hereinafter referred to as "**UK DPA**"), this refers to the UK Data Protection Act 2018.

The Processor guarantees the Controller that it will fulfil the Principal Agreement and this Agreement in accordance with the following terms.

Medloop Ltd.
24 Old Queen Street,
London, SW1H 9HP

Section 1 Scope and definitions

1) The following provisions shall apply to all services of data processing provided by the Processor on behalf of the Controller under EU GDPR/UK GDPR, which the Processor performs on the basis of the Principal Agreement.

2) If this Agreement uses the term "**data processing**" or "**processing**" of data, this shall be generally understood to mean the use of personal data. Data processing or the processing of data shall mean any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

3) Reference is made to further definitions set out in Article 4 of the EU GDPR and UK GDPR.

4) The term "**system**" referred to within this agreement means the main EMIS or SystmOne/TPP electronic systems that a Controller may use, or the HUB available for these; or any electronic system that a Controller uses to record and process patient records.

Section 2 Subject matter and duration of the data processing

1) The Processor shall process personal data on behalf and in accordance with the instructions of the Controller.

2) The data processing shall involve the following primary purpose of carrying out direct patient care through optimisation of patient chronic condition annual reviews via the System CSV extraction of relevant disease register, bulk SMS of patients, telephone outreach to patients as appropriate, and collection of pre-visit information using online questionnaires, and SNOMED code mapping into the System after clinician approval as agreed upon in the Principal Agreement.

3) The duration of this Agreement and any subsequent additions shall correspond to the duration of the Principal Agreement.

Section 3 Nature and purpose of the data processing

1) The nature and purpose of the processing of personal data by the Processor is specified in the Principal Agreement. The Principal Agreement includes the following activities and purposes that may be applicable:

- The Controller transmits relevant data as follows: relevant disease register record data is transmitted via the the System CSV extraction and sent via a secure file sharing service such as NHS Egress. This data is uploaded to the Medloop app. The data is stored in a virtual private cloud (VPC) that is closed to the internet and does not allow routing in or out of the internet and data is encrypted with server-side encryption that does not allow direct access by the data processor employees. Only necessary data as defined by the controller is extracted, which for direct patient care would include a limited number of patient demographic data such as (mobile number, email, NHS number, The System number, date of birth, consultation data, and prescription data.) Data extracts will also go through an initial parallel clinical validation process by comparing The System reporting extracts against the Medloop queries to validate quality as defined by the controller.
- For direct care, then the Processor contacts the patients via SMS message using AWS Pinpoint services. The SMS link is unique to each patient and contains a required link pointing to a survey questionnaire on Medloop's internal App that is hosted on AWS S3 that is on a VPC.
- The patient response is then stored in the aforementioned AWS server of the processor and prioritised via the clinical guidelines set forth by the Controller.
- Data is transferred over an encrypted wire only with access to data by authorised users only.
- To properly connect the patient questionnaire feedback to their The System data, an individualised form link is sent to each patient and their responses are then matched to their NHS number. DOB and phone number as entered by the patient is then used to validate their identity.
- For relevant patients, they are invited, using the SMS services of AWS Pinpoint to book an appointment via the Medloop calendar integration provided via a browser link at the end of the survey questionnaire. These appointments are booked into the Medloop calendar and conducted by qualified personnel, such as Nurse or Clinical Pharmacist, using the Medloop video platform following the Controller's protocols for conducting remote nurse reviews.
- Medloop will not record or store any video consultations, nor the patient’s IP address.
- Survey data is then SNOMED mapped into the System after approval by the controller using either direct data entry of the certified nurse using the remote review guidelines of the controller or via the System Practice IM integration. This data will be stored as a patient consultation.

- To support and increase the take-up rate for the patient survey questionnaire responses, Medloop may provide a patient contact service which will be undertaken via telephone or SMS using relevant information extracted from the System. This will be undertaken by Medloop located in the UK and EEA, trained in confidentiality and data protection as outlined in sect. 10.

2) Additional activities or functionality associated with the processing may be developed during the period of the Principal Agreement. These will be discussed with the Controller and where these comprise significant variation to the activities and processing outlined above, an addendum to the Data Processing Agreement will be provided.

Section 4 Categories of data subjects

The categories of individuals affected by the processing of personal data under this Agreement ("data subjects") include the following.

- Clinically relevant patients as defined by the Controller and NHS QOF Business Rules for relevant disease categories.

Section 5 Types of personal data

The following types of personal data shall be processed under this Agreement:

- Patient name, date of birth, contact details;
- EMIS/SystmOne/TPP or other System number, NHS number, registration status;
- relevant coded data related to the nature of a specific chronic disease such as diagnosis, dates, investigations, and measurements. This would include numerical results for blood test, peak flows, BMI). It would also include relevant medication information such drug names, doses, quantities, and issue dates.

This is a combination of personal data and special category data as defined in Articles 4(1) and 9(1) of the EU GDPR and UK GDPR.

Section 6 Lawful bases for processing

The lawful bases for this service provision with the Controller are Article 6 of the UK and EU GDPR as follows:

- 6(1)(b) Necessary for the performance of a contract to which the data subject (Patient) is party to; and

- 6(1)(e) Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The lawful bases of processing patient health data for the provision of disease registration analysis and health care of patients are in accordance with the nature and purpose of processing as outline in Section 3 and, described in Articles 6 (personal data) and 9 (special category personal data) of the EU GDPR and UK GDPR as follows:

- 6(1)(a) Data subject (patient) has given consent to the processing of his or her personal data for the specified purposes;
- 6(1)(e) Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- 9(2)(a) Data subject (patient) has given explicit consent to the processing of the personal data; and
- 9(2)(h) Necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care, or treatment or the management of health or social care systems and service.

Section 7 Rights and duties of the Controller

1) The Controller is solely responsible for assessing the lawfulness of the data processing and for safeguarding the rights of data subjects and is hence a controller within the meaning of Article 4(7) EU GDPR and UK GDPR.

2) The Controller is entitled to issue instructions concerning the nature, scale, and method of data processing. Upon request by the Processor, the Controller shall confirm verbal instructions immediately in writing or in text form (e.g. by email) to the Processor.

3) Insofar as the Controller deems it necessary, persons authorised to issue instructions may be appointed. The Processor shall be notified of such in writing or in text form. In the event that the persons authorised to issue instructions change, the Controller shall notify the Processor of this change in writing or in text form, naming the new person in each case.

4) The Controller shall notify the Processor immediately of any errors or irregularities detected in relation to the processing of personal data by the Processor.

Section 8 Duties of the Processor

(1) Data processing

The Processor shall process personal data exclusively in accordance with this Agreement and/or the underlying Principal Agreement and in accordance with the Controller's instructions.

(2) Data subjects' rights

a. The Processor shall, within its capabilities, assist the Controller in complying with the rights of data subjects, particularly with respect to rectification, restriction of processing, deletion of data, notification, and information. When the Processor does process personal data specified under Section 5 of this Agreement on behalf of the Controller and these data are the subject of a data portability request under Article 20 EU GDPR and UK GDPR, the Processor shall, upon request, make the dataset in question available to the Controller within a reasonably set time frame, in a structured, commonly used, and machine-readable format.

b. If so instructed by the Controller, the Processor shall rectify, delete, or restrict the processing of personal data specified under Section 5 of this Agreement. The same applies if this Agreement stipulates the rectification, deletion, or restriction of the processing of data.

c. If a data subject contacts the Processor directly to have his or her personal data specified under Section 5 of this Agreement rectified, deleted or the processing restricted, the Processor shall forward this request to the Controller immediately upon receipt.

(3) Monitoring duties

a. The Processor shall ensure, by means of appropriate controls, that the personal data processed on behalf of the Controller are processed solely in accordance with this Agreement and/or the Principal Agreement and/or the relevant instructions.

b. The Processor shall organise its business and operations in such a way that the data processed on behalf of the Controller are secured to the extent necessary in each case and protected from unauthorised access by third parties.

c. The Processor confirms that it has appointed a Data Protection Officer in accordance with Article 37 EU GDPR and UK GDPR and, if applicable, in accordance with the UK DPA, and that the Processor shall monitor compliance with data protection and security laws.

(4) Information duties

a. The Processor shall inform the Controller immediately if, in its opinion, an instruction issued by the Controller violates legal regulations or legislation. In such cases, the Processor shall be entitled to suspend execution of the relevant instruction until it is confirmed or changed by the Controller.

b. The Processor shall assist the Controller in complying with the obligations set out in Articles 32 to 36 EU GDPR and UK GDPR taking into account the nature of processing and the information available to the Processor.

(5) Location of processing

The processing of the data shall in principle take place in the UK. This may be extended to the territory of the Federal Republic of Germany, a member state of the European Union or in another contracting state of the Agreement on the European Economic Area (EEA). Any transfer to a third country outside the EEA may only take place if the special requirements of Article 44 et seqq. EU GDPR and UK GDPR are fulfilled.

(6) Deletion of personal data after order completion

After termination of the Principal Agreement, the Processor shall delete or return all the personal data processed on behalf of the Controller to the Controller after the end of the provision of services relating to processing and delete existing copies, provided that the deletion of these data does not conflict with any statutory storage obligations of the Processor. The deletion in accordance with data protection and data security regulations must be documented and confirmed upon request to the Controller.

(7) Data Quality

The Processor shall notify the Controller of any data quality issues where possible.

Section 9 Monitoring rights of the Controller

1) The Controller shall be entitled, after prior notification in good time and during normal business hours, to carry out an inspection of compliance with the provisions on data protection and the contractual agreements to the extent required, either himself or through third parties, without disrupting the Processor's business operations or endangering the security measures for other Controller and at his own expense. Controls can also be carried

out by accessing existing industry-standard certifications of the Processor, current attestations, or reports from an independent body (such as auditors, external data protection officers or external data protection auditors) or self-assessments. The Processor shall offer the necessary support to carry out the checks.

2) The Processor shall inform the Controller of the execution of inspection measures by the supervisory authority to the extent that such measures or requests may concern data processing operations carried out by the Processor on behalf of the Controller.

Section 10 Sub-processing

1) The Controller authorises the Processor to make use of other processors in accordance with the following subsections in Section 10 of this Agreement. This authorisation shall constitute a general written authorisation within the meaning of Article 28(2) EU GDPR and UK GDPR.

2) The Processor currently works with the subcontractors specified in Annex 2 and the Controller hereby agrees to their appointment.

3) The Processor shall be entitled to appoint or replace other processors. The Processor shall inform the Controller in advance of any intended change regarding the appointment or replacement of other processors. The Controller may object to an intended change.

4) The objection to the intended change must be lodged with the Processor within 2 weeks after receipt of the information on the change. In the event of an objection, the Processor may, at his own discretion, either provide the service without the intended change or propose an alternative subcontractor and coordinate it with the Controller. Insofar as the provision of the service is unreasonable for the Processor without the intended modification - for example, due to the associated disproportionate costs for the Processor - or the agreement on an alternative subcontractor fails, the Controller and the Processor may terminate this Agreement as well as the Principal Agreement with a notice period of one month to the end of the month.

5) A level of protection comparable to that of this Agreement must always be guaranteed when other processors are involved. The Processor is liable to the Controller for all acts and omissions of other processors it appoints.

Section 11 Confidentiality

1) The Processor is obliged to maintain confidentiality when processing data for the Controller.

2) In fulfilling its obligations under this Agreement, the Processor undertakes to employ only employees or other agents who are committed to confidentiality in the handling of personal data provided and who have been appropriately familiarised with the requirements of data protection. Upon request, the Processor shall provide the Controller with evidence of the confidentiality commitments.

3) Insofar as the Controller is subject to other confidentiality provisions, it shall inform the Processor accordingly. The Processor shall oblige its employees to observe these confidentiality rules in accordance with the requirements of the Controller.

Section 12 Technical and organisational measures

1) The technical and organisational measures described in Annex 1 are agreed upon as appropriate. The Processor may update and amend these measures provided that the level of protection is not significantly reduced by such updates and/or changes.

2) The Processor shall observe the principles of due and proper data processing in accordance with Article 32 in conjunction with Article 5(1) of the EU GDPR and UK GDPR. It guarantees the contractually agreed and legally prescribed data security measures. It will take all necessary measures to safeguard the data and the security of the processing, in particular taking into account the state of the art, as well as to reduce possible adverse consequences for the affected parties. Measures to be taken include, in particular, measures to protect the confidentiality, integrity, availability and resilience of systems and measures to ensure continuity of processing after incidents. In order to ensure an appropriate level of processing security at all times, the Processor will regularly evaluate the measures implemented and make any necessary adjustments.

Section 13 Liability/Indemnification

1) The Processor shall be liable to the Controller for any and all loss or damage culpably caused in the performance of the services under the Principal Agreement or by a breach of applicable statutory data protection obligations on the part of the Processor, its employees or parties commissioned by it to implement the Principal Agreement.

2) The Processor shall not be obliged to pay compensation if the Processor proves that it has processed the data provided by the Controller solely in accordance with the instructions of the Controller and that it has complied with its obligations arising from the EU GDPR and UK GDPR specifically directed to processors.

3) The Controller shall indemnify the Processor against any and all claims for damages asserted against the Processor based on the Controller’s culpable breach of its own

obligations under this Agreement or under applicable data protection and security regulations.

Section 14 Miscellaneous

1) In case of contradictions between the provisions contained in this Agreement and provisions contained in the Principal Agreement, the provisions of this Agreement shall prevail.

2) Amendments and supplements to this Agreement shall be subject to the mutual consent of the contracting parties, with specific reference to the provisions of this Agreement to be amended. Verbal side agreements do not exist and shall also be excluded for any subsequent changes to this Agreement.

3) The Agreement (including any non-contractual matters and obligations arising from it) shall be governed by and construed in accordance with the law of England. Any dispute, controversy, proceedings or claim between the parties relating to the Agreement (including any non-contractual matters and obligations arising from them) shall fall within the exclusive jurisdiction of the courts of England.

4) In the event that access to the data which the Controller has transmitted to the Processor for data processing is jeopardised by third-party measures (measures taken by an insolvency administrator, seizure by revenue authorities, etc.), the Processor shall notify the Controller of such without undue delay.

5) In addition and subsequent to a request, the following specific wording from the UK Information Commissioner's website has been included to further expand on the above clauses:

- The Data Protection Act 2018 and UK and EU GDPR as enacted gives the right to individuals to access Personal Data held about them, the right to know how their data is being used and the right to object to the way their data is being used. The Controller shall notify the Processor if a request for Personal Data has been submitted by a Data Subject. The Processor shall assist the Controller and provide full co-operation in the process of responding to any request for Personal Data made by the Data Subject within the legislated timescales. The Processor shall not disclose or respond to the Data Subject's request for Personal Data other than at the request of the Controller.

- Following an actual or suspected breach of personal data the Processor will, within 72 hours of becoming aware of the breach, make the following information available to the Controller:
  - The nature of the breach;
  - The scale of the breach;
  - The perceived risk associated with the breach;
  - The measures taken to deal with and mitigate the effects of the breach.

- Depending on the above, it may then be necessary for the Controller to inform the Information Commissioner's Office (ICO), and to put further processes, technical measures and/or system fix(es) in place to prevent further loss of confidentiality, integrity and/or availability. Following any remedial action the residual risk will be assessed. If the level of residual risk is found to be unacceptably high, further measures will be implemented and the risk re-evaluated. Depending on the nature of the breach it may be necessary to involve third party information security specialists.

Medloop Ltd.
24 Old Queen Street,
London, SW1H 9HP

Schedule of Annexes

Annex 1 Technical and organisational measures taken to ensure the security of processing.
Annex 2 Sub-processors pursuant to Section 9 of this Data Processing Agreement.

Agreement to Data Processing

_____	_____
Place, date	**Place, date**
_____	_____
Signature (Controller)	**Signature (Processor)**

Medloop Ltd.
24 Old Queen Street,
London, SW1H 9HP

Annex 1

Technical and organisational measures to ensure the security of processing.

The Processor guarantees that the following technical and organisational measures have been taken where relevant to the service provision:

A. Pseudonymisation measures

Measures that reduce direct references to persons during processing in such a way that it is only possible to associate data with a specific person if additional information is included. The additional information must be kept separately from the pseudonym by appropriate technical and organisational measures.

Description of the pseudonymisation:

- *First name and last name is removed from data*
- *address data is removed from data*

B. Encryption measures

Measures or operations in which a clearly legible text/information is converted into an illegible, i.e. not easily interpreted, character string (secret text) by means of an encryption method (cryptosystem).

Description of the encryption measure(s):

- *Symmetrical/asymmetrical encryption*
- *Block algorithms (e.g. AES, 3DES)*
- *Stream encryption (A5 algorithm)*

C. Measures to ensure confidentiality

1. Physical access control

Measures that physically deny unauthorised persons access to IT systems and data processing equipment used to process personal data, as well as to confidential files and data storage media.

- *Description of physical access control:*
- *Controlled key assignment: Medloop office has a controlled key assignment only to registered staff and approved maintenance personnel*
- *Door protection (electronic door opener, etc.)*

- *Monitoring device (alarm systems, video surveillance)*
- *Secured server room*
- *Control system for visitors*

2. Logical access control

Measures to prevent unauthorised persons from processing or using data which is protected by data privacy laws.

Description of logical access control system:

- *Password procedure, i.e. personal and individual login user credentials when logging on to the system (e.g. special characters, minimum length, regular password change)*
- *Automatic locking after a certain time interval (e.g. password or pause switching)*
- *Limitation of the number of authorised employees*
- *Access lists*
- *Isolation of sensitive systems through separate network areas*
- *Authentication procedures*
- *Regularly updated antivirus and spyware filters*

3. Data access control

Measures to ensure that persons authorised to use data processing systems can only access personal data according to their access rights, so that data cannot be read, copied, changed or removed without authorisation during processing, use and storage.

Description of data access control:

- *Authorisation concepts (profiles, roles, etc.) and their documentation*
- *Logging*
- *Archiving concept*
- *Logging of access and abuse attempts*
- *Google sheets maintains a log of users access attempts and blocks non-authorised users (for Medloop)*
- *Google forms maintains an original copy of patient survey responses that is not permanently editable (for Medloop)*
- *NHS Smartcard allocation*

4. Separation rule

Measures to ensure that data collected for different purposes are processed separately and separated from other data and systems in such a way as to preclude the unplanned use of such data for other purposes.

Description of the separation control process:

- *Authorisation concepts with regards to user permission and access controls*
- *Encrypted storage of personal data*
- *Software-based customer separation*

D. Measures to ensure integrity

1. Data integrity

Measures to ensure that stored personal data cannot be corrupted by means of a malfunctioning of the system.

Description of data integrity:

- *Logging*
- *Transport processes with individual responsibility*

2. Transmission control

Measures to ensure that it is possible to verify and establish to which bodies personal data may be or have been transmitted or made available using data communication equipment.

Description of transmission control:

- *Logging*
- *Transport processes with individual responsibility*

3. Transport control

Measures to ensure that the confidentiality and integrity of data is protected during transmission of personal data and transport of data carriers.

Description of transport control:

- *Transmission of data via encrypted data networks or tunnel connections (VPN)*
- *Transport processes with individual responsibility*
- *Comprehensive logging procedures*

- **System** *report extract data will be shared with Medloop using Egress, NHSmail's encryption service (where applicable)*
- **System** *bulk extract will be shared with Medloop using a secure HSCN connection provided by hSo (where applicable)*
- **System** *Hub data shared by unique login and access*

4. Input control

Measures to ensure that it can be subsequently verified and ascertained whether and by whom personal data have been entered or modified in data processing systems.

Description of the input control process:

- *Logging of all system activities and keeping of these logs for at least three years*

E. Measures to ensure availability and resilience

1. Availability control

Measures to ensure that personal data are protected against accidental destruction or loss.

Description of the availability control system:

- *Mirroring of hard disks*
- *Uninterrupted power supply*
- *Fire alarm system*
- *Air conditioning*
- *Alarm system*
- *Emergency plans*
- *No water-bearing pipes above or near server rooms*
- *Google ensures backup of stored data (for Medloop)*
- *AWS ensures backup of stored data (for Medloop)*

2. Quick recovery

Measures to ensure the ability to quickly restore the availability of and access to personal data and used systems in the event of a physical or technical incident.

Description of the measures for quick recovery:

- *Emergency plans: Google sheets always maintains an original copy of patient survey responses*

- *AWS makes automatic data snapshots that we can recover the data from*

3. Reliability

Measures to ensure that the functions of the system are available and malfunctions are reported.

Description of measures for reliability:

- *Automatic monitoring with email notification*
- *Emergency plans with responsibilities*

F. Measures for the regular testing and evaluation of the security of data processing

1. Verification process

Measures to ensure that the data are processed securely and in compliance with data protection regulations.

Description of verification process:

- *Data protection management*
- *Regular re-certification*
- *Formalised processes for data privacy incidents*
- *Documentation of instructions received by the Controller*
- *Formalised order management*
- *Service level agreements for carrying out controls*

2. Order control

Measures to ensure that personal data processed on behalf of the Controller can only be processed in accordance with the instructions of the Controller.

Description of the order control measures:

- *Instructions from the Controller are documented*
- *Data is reviewed by a clinical resource approved by the Controller prior to taking any clinical action when necessary*

Medloop Ltd.
24 Old Queen Street,
London, SW1H 9HP

Annex 2

Sub-processors pursuant to Section 9 Data Processing Agreement

The Processor currently works with the following subcontractors for their business and the Controller hereby agrees to their appointment.

Company: Google Ireland Limited

Data processing activity	Store Google Forms based data (data details see section 3)
Company Location	Gordon House, Barrow Street Dublin 4, Ireland
Data Location	Ireland or European
Google states full GDPR compliance for data handling	https://cloud.google.com/security/gdpr?hl=de
Privacy policies	https://policies.google.com/privacy?hl=de
Google also offers privacy removal request forms for GDPR compliant data handling	https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf
Google confirms that there is no access possible to the stored data for any Google employee.	

Company: HighSpeed Office (hSo)

Data processing activity	Provides HSCN connection
Company Location	50 Leman Street, London, E1 8HQ
Data Location	London Data Centre
hSo is an official partner of the NHS and has achieved HSCN Stage 2 Compliance	https://www.hso.co.uk/company/news/hso-achieves-hscn-stage-2-compliance-to-support-health-and-social-care-organisations

Medloop Ltd.
24 Old Queen Street,
London, SW1H 9HP

Company: Amazon Web Services EMEA SARL

Data processing activity	Store cell phone number and IP address when Amazon Video Call service when used for video consultations
Company Location	38 avenue John F. Kennedy, L-1855 Luxembourg
Data Location	London Data Centre
AWS states full GDPR compliance for data handling	https://aws.amazon.com/de/compliance/germany-data-protection/
Privacy policies	https://aws.amazon.com/de/compliance/data-privacy/
AWS confirms that there is no access possible to the stored data for any AWS employee. AWS also guarantees that the data is not leaving (for backup or availability) the selected region – in our case the London data Centre.	

Company: Twilio

Data processing activity	Integrated telephony solution
Company Location	Global – London Office – 100 New Bridge street, London, EC4V 6JA
Data Location	London / EU Data Centre
Twilio states full GDPR compliance for data handling	https://www.twilio.com/gdpr
Privacy policies	https://www.twilio.com/legal/privacy
Twilio holds ISO27001 certification, and SOC2 reports. Twilio provides a range of legal agreements and policy statements on their website which are compliant with UK and EU legislation.	

Company: Medloop Technologies GmbH

Data processing activity	Technical Support. Manage contracts and client contact.

Medloop Ltd.
24 Old Queen Street,
London, SW1H 9HP

Company Location	Brunnenstr. 141a, 10115 Berlin, Federal Republic of Germany UK office (Registered and Postal Address) – 24 Old Queen Street, London, SW1H 9PH
Data Location	London Data Centre
Medloop states Certification to demonstrates security compliance	https://medloop.co/certifications/
Privacy policy	https://medloop.co/privacy-policy/
Medloop Technologies GmbH is acting in full compliance with EU GDPR. Medloop Technologies GmbH is ISO 27001 certified and registered on the DSPT.	