DATA PROTECTION POLICY BASIC FRAMEWORK

This Policy contains rules that LLcloud Ltd., UIC 206851771 is obliged to comply with daily in view of the requirements of the applicable legislation on personal data protection including the General Data Protection Regulation (GDPR).

2021

Introduction

This General Personal Data Protection Policy (**"Policy"**) is used by LLcloud Ltd. (hereinafter referred to as "**LLCLOUD**" or the "**Company**") in compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons as regards the personal data processing and the free movement of such data and the repealing of Directive 95/46 / EC (GDPR) (the **"General Data Protection Regulation"** or just the **"Regulation"**) and the provisions of other applicable data protection legislation.

The words **"we"**, **"our"** etc. in this document refer to LLcloud Ltd. unless otherwise inferred by the context .

For the meaning of uppercased terms and abbreviations used in this document, please see the "Definitions" section at the end of the document.

The Importance of Personal Data Protection for Us

The personal inviolability of our team, customers, partners, contractors and other natural persons whose personal data is processed by LLCLOUD in the course of its activity is extremely important for us. The protection of the personal data of those persons and their use in a conscientious and lawful manner is of prime importance for LLCLOUD values and for our reputation and is a key element in maintaining our relationships with our customers and partners.

Purpose of the Policy

This Policy is aimed at facilitating the practical application of the legislation on personal data protection by the Company and our Team by describing the principles and procedures that LLCLOUD is committed to observe in carrying out its activity in compliance with the personal data legislation and our team's responsibilities in personal data processing.

The policy is aimed at preventing the illegal or unscrupulous personal data processing (e.g. unauthorized disclosure, storage, modification or destruction of personal data).

Scope

This Policy is part of LLCLOUD's internal rules and procedures and applies to all personal data processed by the Company: both personal data processed (a) in full or partially by automatic means and (b) on paper.

The policy applies to the LLCLOUD Manager as well as to the LLCLOUD team (which for the purposes of these Rules includes persons working for the Company under employment contracts or part-time (referred to as the **"team"**). The LLCLOUD Manager is responsible for the implementation of the Policy in the LLCLOUD activity and for guaranteeing its observance as well as the compliance with the personal data legislation by the entire team.

The deliberate or negligent non-compliance with this Policy and with other internal rules related to the personal data processing and the personal data legislation by the employees of the company or by persons working for it under contracts equivalent to employment contracts is a violation of the discipline at work and is a reason for taking disciplinary measures by LLCLOUD pursuant to the

Labor Code. Moreover, a violation of the rules related to the personal data protection by the respective employees may in certain cases result in criminal liability.

This Policy is observed parallel to the applicable personal data legislation whereas the latter has priority over the Policy in the event of a contradiction or when the personal data legislation stipulates stricter rules.

If the personal data legislation requires a review of this Policy it shall be reviewed and updated accordingly.

Principles of Personal Data Protection

We, at LLCLOUD declare that we shall do our best to fulfil our obligations arising out of the personal data legislation and shall fully comply with the principles below and other basic regulatory requirements regarding personal data protection (jointly referred to as the **"Principles"**).

Principle 1: Legality

We shall process personal data only if there are *legitimate grounds* for it set forth in the personal data legislation. We process personal data legally when such processing is necessary for:

- our (or a third party's) ***legitimate business interest***: for instance our legitimate interest is to perform tests which is our obligation under a contract with our customer. However we cannot rely on the legitimate interest grounds when the interests or fundamental rights and freedoms of the Subjects of the data processed take precedence over that interest and especially when the Data Subject is a child;
- compliance with ***our legal obligation*** (e.g. for taxation purposes or for notifying the relevant state authorities in the event of an incident) or
- ***the implementation of a contract*** which we have concluded with the Data Subject as well as for taking action at the request of the Subject before signing a contract (e.g. in order to perform a test we should have the names of the person who will perform the test).

The personal data processing is carried out with the ***consent*** of the respective Subject. We may as an exception process personal data on any of the above grounds whenever that is possible as a last resort and insofar as it may not be possible to obtain a valid consent due to the stricter requirements of the Regulation. However consent shall be required for the use of cookies and similar technologies on the Company's website for registering a user's account when uploading or downloading data in performing tests, etc.

N.B.:

- Each member of our team shall make sure that there are legal grounds for any processing of personal data he/she is responsible thereof.
- If it is necessary to request additional personal data or to change the way personal data are processed we shall always check whether there are legal grounds thereof.
- In case personal data are provided by a Data Subject to LLCLOUD without legal grounds under Art. 6, para 1 of the Regulation or at variance with the principles under Art. 5 of the

same Regulation within one month of learning it LLCLOUD shall be obliged to return them and if that is impossible or requires a disproportionately great effort - to delete or destroy them. Deletion and destruction shall be documented by a protocol of the Manager.

- LLCLOUD may copy an identity document, a driving license or a residence document only if that has been stipulated by law. In all cases where the copying of the those documents has not been stipulated by law LLCLOUD may request them from the Personal Data Subjects only to verify their identity and the accuracy of the spelling of their personal data if such a need arises and then return them without copying or scanning them.

- LLCLOUD does not provide free public access to information containing a unique identity number or a personal number of a foreigner.

- LLCLOUD takes appropriate technical and organizational measures that do not allow the unique identity number or the personal number of a foreigner to be the only means of identification of the user when being provided with a remote access to the relevant electronic service. For instance individuals who wish to log in to the LLcloud system register both by entering a username or an email and a password. LLCLOUD does not require or collect any PIN or PIC from them.

Principle 2: Good Faith and Transparency

In order to be meticulous and transparent in our personal data processing activities we must earnestly and in a clear and accessible way explain to natural persons how we process their data by using simple language (avoiding special terms as far as possible). That information shall include what personal data we collect, how we intend to use them, with whom we can share them if we intend to transfer them to countries outside the European Economic Area ("**EEA**"), and how individuals can contact the LLCLOUD for questions or for exercising their rights.

We provide the above information to our customers, to persons wishing to participate in tests and to employees in a document called a *Confidentiality Notice* and to visitors of our website - through our *Cookies Policy*.

N.B.:

- If it is necessary to request additional personal data or to change the way of personal data processing we shall always consider whether additional information must be provided to the relevant Subjects. Particular attention shall be paid to informing natural persons about the use of their data for purposes which they have not expected.

Principle 3: Limitation of Purposes

Personal data may only be used for the purposes for which the data have been collected. We shall not use personal data for purposes about which the natural person has not been notified or which are not obvious to the person (or are incompatible with the original purpose). For example:

- the employee should disclose personal data to other persons only when those other persons need them in order to perform their functions or tasks, i.e. when the person should have the data in question so as to carry out his/her tasks;

- in order to determine whether the new processing purpose is compatible with the original purpose for which the data have been collected, the team should consider whether those purposes are related, the circumstances in which personal data have been collected and the relationship between persons, the nature of the personal data, the possible consequences of future data processing and potential security measures;

Principle 4: Data Minimization

The personal data we collect must be relevant and limited to the minimum needed for the purposes of data collection. We shall not request more personal data than we need in view of the legal grounds on which we collect them. We shall carry out checks on the relevance of the personal data collected by our Team to guarantee the LLCLOUD activity compliance with this principle.

We take into account the following data minimization techniques where their use is possible and appropriate:

- **Less is more**: we shall always ask ourselves the question: do we need to collect this information to achieve our goals? An example of excessive collection of personal data is the sending of a general questionnaire to those wishing to test a sensor and the software for it. That questionnaire includes specific questions about the applicant's family and/or work, which are not needed for the concrete case of that applicant's assessment.
- **Pseudonymisation:** means personal data processing in such a way that the data could no longer be related to a concrete Subject without additional information provided that the additional information is stored separately and that technical and organizational measures have been taken to guarantee that the data cannot be related to a concrete natural person. Example: the name and PIN identifier in a definite database is replaced by a code and the information about which code and which name/PIN corresponds to it is stored separately.

Principle 5: Data Accuracy

Personal data should be accurate and up-to-date. We shall urge natural persons to inform us about any changes as regards their personal data (and we shall update, correct or delete our records accordingly).

N.B.:

- We shall not use personal data suspected to be out of date without confirming their accuracy.
- We shall guarantee the accurate recording and management of personal data in the relevant systems. Irrelevant or obsolete information shall be removed and destroyed in compliance with our *Policy on the storage and destruction of documents and information containing personal data*.
- If we have been notified of a change in the data of a customer or of some of our counterparties the respective database shall be updated without delay.

Principle 6: Limitation of Storage

Personal data shall not be stored longer than necessary for achieving the legitimate aim for which they have been collected. Once the aim has been achieved the data should be destroyed in a secure manner. This requirement may be adjusted pursuant to the provisions of other laws stipulating that we keep the information for a longer period of time. In some cases that may be likewise required by our legitimate interest. For more details see the *Policy on the storage and destruction of documents and information containing personal data*.

If for some reason personal data cannot be destroyed or deleted (or anonymized) this principle shall be observed if the information "has been disposed" provided that we:

- are unable or shall not use personal data to make decisions related to the Data Subject or in any other way that may affect the Subject;
- restrict the personal data access by appropriate technical and organizational measures; and
- undertake to carry out the final destruction of the data in a secure manner if and when that becomes possible.

Principle 7: Data Integrity and Confidentiality

Personal data shall be stored and used in a secure manner. Data need to be protected against unauthorized or illegal processing and against accidental loss, damage or destruction. This applies to our information systems, websites and the daily data processing performed by us. We shall at least comply with any security measures required by law.

Some of the security measures we have taken include: preventing data loss; password rules; anti-malware to mention but a few.

Selecting Data Processors

If LLCLOUD (as an administrator) engages another organization to process personal data on our behalf that organization ("data processor") must have taken "appropriate technical and organizational measures" to meet the requirements of the applicable personal data law and to guarantee the protection of natural persons' rights. As part of this process we shall conclude a written contract with the data processor. Its content shall be complied to the requirements of law.

Within the framework of what has been agreed between LLCLOUD and the data processors pursuant to art. 28 of the Regulation we shall inspect our processors (and possibly the processing subcontractors) and in particular their systems, registers, premises, team and other resources related to the provision of the relevant services so as to guarantee that the data processors comply with their contractual obligations and the applicable data protection legislation.

Principle 8: Data Transfers outside the EEA

- Personal data legislation restricts personal data transfer outside the EEA (including transfers to companies in their capacity of data processors) unless when there is sufficient protection of personal data or appropriate measures taken to guarantee data protection. LLCLOUD may in

rare cases transfer data to persons outside the EEA which shall be done in compliance with standard contractual clauses approved by the EC regulating certain data transfers between us and other companies.

In a limited number of other cases personal data may also be transferred outside the EEA namely when:

- the data are sent to a country or to an international organization recognized by the European Commission (EC) by applying adequate protection measures (including American organizations certified under the *Personal Data Shield in EU-US Relations*);
- relying on binding corporate rules;
- relying on standard data protection clauses adopted or approved by the European Commission;
- the Subject has given an explicit consent for the transfer;
- that is necessary for the implementation of a contract between the data subject and the LLCLOUD;
- that is necessary for reasons of major public interest; or
- that is required for filing, exercising, or defending against a legal claim.

Principle 9: Respect for Data Subjects's Individual Rights

We shall always respect the rights of natural persons granted to them by personal data legislation, including (and where applicable) the right to:

- be provided with information on how their personal data are processed (for more details see *Principle 2: Integrity and Transparency* above);
- have their personal data supplemented and corrected;
- have their data deleted or their processing limited upon request;
- have their personal data transfered to another administrator upon request;
- object to the processing based on the legitimate interest of LLCLOUD or of a third party or on the direct marketing carried out in relation to them (including profiling related to direct marketing);
- avoid being the subject of fully automated decisions (including profiling) that may give rise to legal consequences or significantly affect natural persons.

We shall respond to any request timely and normally within one month as of the date of receiving it as it has been set forth in our *Policy on the Exercise of the Rights of Data Subjects and Responding to Third Party Requests for Disclosure of Personal Information*.

Principle 10: Accountability

- We shall take a wide range of measures aimed at reducing the risk of non-compliance with that principle and at demonstrating that we take seriously the protection of personal data. Some of these measures are described below.

Registers of data processing activities

Prior to the implementation of the Regulation (May 25, 2018) the Personal Data Protection Act required that the Administrators must register their data processing activities with the CPDP. With the entry into force of the Regulation we are obliged to maintain registers of our personal data processing which contain a description, inter alia, of the categories of personal data and the grounds for their processing, the setting forth of positions related to data processing and data protection. Those registers should be submitted to the CPDP upon request.

Team training

Upon engagement in LLCLOUD the employees shall read this Policy and declare that they shall comply with it. Employees who process personal data as an essential part of their job description shall receive appropriate instructions and training on data protection as well as periodical instruction and training of the Team thereof.

New systems and processes

Personal data legislation requires that we take into account and apply data protection measures in our data processing activities known as the Privacy by Design Principle and the Privacy by Default Principle.

We adhere to the above principle by:

- identifying the risks for the personal inviolability at the very beginning of each new project and before the introduction of a new system, product or service and the planning of actions aimed at addressing them;
- following the principle of data minimization including the application of data pseudonymisation where possible and justified from a business point of view;
- respecting personal inviolability in designing and using our technologies, actions and processes and consultating with all interested persons;
- maintaining high standards of our products and services; and
- striving to be transparent to natural persons about what we do to protect their personal data.

Impact assessment

In January 2019 LLCLOUD performed an analysis and assessment of the level of risk for personal data protection according to which the personal data processing by the Company in view of the nature, scope, context and purposes of the processing shall not pose a high risk for the rights and freedoms of natural persons.

However, if at a certain moment a probability of "a high risk" arises during the processing or LLCLOUD starts to perform any of the processing operations specified by the CPDP in the "List of types of personal data processing operations which need an assessment of the impact on data protection pursuant to Art. 35, para 4 of Regulation (EC) 2016/679"[1], the relevant operations should be subjected to a more thorough analysis and assessment (the so-called "Data protection impact assessment") in compliance with the requirements of the Regulation.

The impact assessment should include a description of the processing activities, the risks arising thereof and the measures taken to alleviate those risks and in particular guarantees and security measures related to data protection the compliance with the Regulation. In a limited number of cases (for instance if the Impact assessment shows a high residual risk for the rights and freedoms of the Subjects) we may have to consult the relevant natural persons or the CPDP.

Any new product, system or service created or purchased by us that involves the processing of personal data which: (i) are not of the type processed so far; or (ii) have not been used in this way before; or (iii) the processing of such data may be perceived by our customers, employees or other natural persons as threatening their personal inviolability, then an analysis should be made to determine whether such processing affects the rights and freedoms of the relevant natural persons and whether the processing should be assessed as posing a "high risk".

Internal audits

We shall check regularly the compliance of the Data Processing activities with the above principles and with the personal data legislation by internal audits. All members of our team shall provide assistance for the implementation of those audits.

Assistance to the CPDP

Upon request LLCLOUD shall provide assistance to the CPDP in the performance of its tasks and powers. When in the exercising of its powers the CPDP may violate the LLCLOUD obligation to protect professional secrecy or any other obligation related to secrecy keeping stipulated by law LLCLOUD shall refuse to provide an access to the information protected as a secret.

Obligations and Responsibilities of the Team

Our team members have the following responsibilities related to personal data protection:

(1) to be familiarized with the current LLCLOUD Policies and other internal acts related to personal data protection including internal instructions and guidelines;

(2) to participate in briefings and trainings on personal data protection organized by the Company;

(3) to keep the confidentiality of personal data to which they have an access or which have become known in the process of or in connection with the performance of their duties and not to disclose them to unauthorized third parties including family members, friends and acquaintances and other employees of the administrator. A confidentiality clause thereof has been included in the contracts with all team members;

---

[1] The list is published on the website of the CPDP - https://www.cpdp.bg/?p=element&aid=1186

(4) not to use personal data to which they have an access in the process of and on the occasion of the performance of their duties for purposes other than for the performance of their duties; in particular they shall not have the right to view and copy paper documents and files on a computer or other electronic medium to which they do not have an authorized access;

(5) to process only personal data necessary for the performance of their concrete work duties;

(6) to notify the LLCLOUD manager in case of any violation of personal data security as well as in case of identifying a potential risk of such a violation;

(7) to comply with the personal data legislation, this Policy and our other internal acts related to personal data protection;

(8) to notify the LLCLOUD manager, their immediate superior and the DPO in cases when they have to process personal data for purposes other than the ones initially set forth.

Video surveillance

LLCLOUD has a legitimate interest in guaranteeing the safety of all test participants which may sometimes be a necessary condition for performing the tests themselves and some parts of them. For that purpose the Company may in rare cases perform video surveillance in public areas by equipping the persons performing the tests with video cameras. The use of video cameras shall be announced by placing warning notices on the persons who use those cameras and the video surveillance thus performed shall be made known through the persons doing it.

You will find more information about the video surveillance performed by the Company in our *Video surveillance control policy*.

Main definitions

For the purposes of this Policy the terms and abbreviations below have the following meaning:

"**Administrator**"	A commercial company or a person who (alone or jointly with other persons) determines the purposes of personal data processing and the manner the data are processed. For instance LLCLOUD is an Administrator as regards the processing of personal data of members of its team, customers and test performers.
"Personal data legislation"	The Regulation on personal data and other acts of the European Union on personal data protection as well as any normative act that implements and/or creates measures for the implementation of those European acts or an additional national regulation on personal data protection in Bulgaria (including PDPA and Regulation No. 1 of 30 January 2013 on the minimum level of technical and organizational measures and the admissible type of personal data protection, guidelines and practice of the CPDP as well as case-law, insofar as they are compatible with the Personal Data

	Regulation) and any other law or normative act that amends, supplements, replaces or consolidates the above mentioned acts.
"The Company"	Is LLcloud Ltd., UIC 206851771; also referred to as "LLCLOUD".
"PDPA"	The Personal Data Protection Act in force (SG, issue 1 of 2002 with subsequent amendments).
"CPDP"	Commission for Personal Data Protection.
"Personal data" or "data"	Refer to any information related to an identified natural person (employee, customer, service provider) or a natural person who can be identified (a) by that information or (b) by that information considered as being related to any other information which the Administrator owns or can acquire. Examples of personal data are: name, address, date of birth, bank account number, opinion about the natural person, video and audio recordings. Anonymous information does not constitute personal data. The fact that certain information is publicly accessible (e.g. via LinkedIn) does not prevent the application of personal data legislation to such information. The natural person may be identified directly or indirectly by a specific identifier such as name, PIN, location, online identifier or by one or more specific factors for the physical, psychological, genetic, economic, cultural or social identity of that natural person.
"Security violation (of data)"	Means a violation of personal data security which results in the accidental and/or unlawful destruction, loss, modification, unauthorized access or disclosure of the data in the process of their storage, transfer or other forms of processing.
"Processing (of personal data)"	Is of a very wide range and includes virtually everything we do with personal data including their acquisition, storage, use in any way (organizing, structuring, adapting or modifying, retrieving, disclosing, transmitting, distributing, etc.) as well as their destruction.
"Processor (of personal data)"	A natural person or a legal entity, public authority or another structure that processes personal data on behalf of the Administrator. Example: an external IT maintenance company providing services for LLCLOUD.
"General Personal Data Regulation" ("the Regulation")	Has the meaning set forth in the *"Introduction"* section above.
"Team"	Has the meaning set forth in the *"Scope"* section above.
"Principles"	Has the meaning set forth in the section *"Personal data protection*

	principles" above.
"Subject (of personal data)"	A natural person who has been identified or can be identified (directly or indirectly) on the basis of any information that may be considered personal data. See also the definition of "personal data". LLCLOUD employees and customers are Subjects (of personal data).
"Special personal data categories"	Personal data that are the subject of special legal protection: these are data revealing racial or ethnic origin, political views, religious or philosophical beliefs or trade union membership as well as the processing of genetic data, biometric data for the sole purpose of identifying a natural person, health data or data related to the sexual life or sexual orientation of the natural person (also referred to as "Sensitive data"). Thus for instance the Team's health information stored by the Company is a "Special data category". The processing of data related to convictions and administrative offenses is further restricted by the applicable laws and is also a "Special data category".

Annex - Security measures

Some of the security measures applied by us at LLCLOUD as regards the protection of personal data are set forth below.

Physical data protection

The company does not operate in a large office and actually more than one team members are very rarely physically present there. Therefore, physical protection, although being of major importance for guaranteeing the information security is not essential due to the nature of the team members' work. Every member of the team actually works alone, is separated from the others and may be even in a different building. The physical protection measures we apply include:

- documents containing personal data are stored in a locked cabinet or security container. If the data are electronic they should be encrypted or password protected both on the hardware device and in the network and should be periodically backed up. If the backup is on a portable storage device, the latter should be stored in a locked cabinet or security container;

- unnecessary copies of paper documents and the like containing personal data should be destroyed by a shredder or by other secure means.

Data Discovery, Cataloguing and Classifying

- In addition to the above we also apply control measures guaranteeing that personal data are processed safely and outside our main systems and we also guarantee the protection of information such as:
- copies of databases, including personal data, for testing, analysis and upgrading;
- e-mail archives that are likely to contain personal data.

Data Loss Prevention

We may use measures for the prevention of data loss such as automatical blocking of outgoing emails and moving of files containing personal data if they have not been properly protected (e.g. by encryption).

In some situations encryption could be automatically applied to personal data when such data have been identified and classified in e-mail messages or attached to e-mail documents while in other cases the messages may be quarantined.

Data and email encryption

Encryption is one of the few techniques explicitly mentioned in the Regulation which in itself urges organizations to apply it. If necessary we shall apply measures for data encryption both statically and when they are used and transmitted. This guarantees that even in the event of a breach in any of our systems the information will remain confidential.

Data portability

As pointed out in Principle 9 on the individual rights of Subjects the latter have the right to request the export of data related to them in an appropriate format that can be provided to another service provider so that the latter may import the data in view of providing services for the Subject. Although the exercise of this right is of low likelihood LLCLOUD uses widely available products (such as Microsoft Office) to facilitate the exercise of this right.

Cloud Storage and Sharing Services

- LLCLOUD shall periodically review documents that are subject to cloud services so as to minimize their sharing with third persons. Transfers of personal data both internally among the Team members and outside the Company should be implemented with due care and attention. Thus for instance when sending an email you must be sure that you are sending the information to the proper recipient and not to a wrong email address.
- Keep in mind that information seekers could sometimes use fraudulent means. Before sending personal data to third parties make sure of their identity especially if you provide information over the phone. If in doubt please contact the LLCLOUD manager.

Anti-Virus and Anti-Malware

The successful penetration of a virus or malware in the computer systems can make them unusable, but even a more serious concern from the point of view of data protection is the possibility for obtaining data about the access to users and to the administrator's accounts as a result of that penetration. In this way access can be obtained to personal data and other confidential information of the Company stored on its devices and in the cloud.

In close collaboration with IT service providers LLCLOUD takes care to provide actually the strongest possible protection against malware by using the most up-to-date anti-virus software.

Data Breach Identification and Blocking

Personal data legislation requires that we notify the CPDP without any delay about personal data security breaches (and where possible within 72 hours) after learning of a personal data security breach (unless the breach is unlikely to jeopardize the rights and freedoms of natural persons).

In certain circumstances we may also have to notify natural persons and document personal data security breaches in compliance with our *Data Security Breaches Policy*.

- If a member of our team becomes aware of a breach of personal data security he/she should immediately notify the LLCLOUD manager and provide for him/her all available information about the case (including the nature and consequences of the breach and the possible measures

taken or to be taken for reducing the negative consequences). Examples of data security breaches are: the incorrect sending of personal data to a recipient other than the recipient who should receive them; unauthorized access to personal data; theft or loss of documents or mobile devices (laptops, external storage, etc.) containing personal data.

Contacts

LLCLOUD's Managing Director

Stavri Nikolov

Stavri.Nikolov@llcloud.eu

LLCLOUD's Technical Team

team@llcloud.eu