Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

the Customer - as described in paragraph 1.2 of the "AGREEMENT REGARDING PRODUCTS AND SERVICES" (https://www.egain.io/gtc)

(the data controller)

and

Kiona Holding AS
CVR 983 190 510
Leirfossvegen 27
7038 Trondheim
Norway

and its subsidiaries

(the data processor)

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 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).

3. In the context of the provision of Kiona Edge and supporting services, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

---

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:
   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

    If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general authorisation of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least one month in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

    The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

    b. transfer the processing of personal data to a sub-processor in a third country

    c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

    This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

    a. the right to be informed when collecting personal data from the data subject
    b. the right to be informed when personal data have not been obtained from the data subject
    c. the right of access by the data subject
    d. the right to rectification
    e. the right to erasure ('the right to be forgotten')
    f. the right to restriction of processing
    g. notification obligation regarding rectification or erasure of personal data or restriction of processing
    h. the right to data portability
    i. the right to object
    j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

    a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, Integritetsskyddsmyndigheten (called Datainspektionen until 2021-01-01), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

    b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

    c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

    d. the data controller's obligation to consult the competent supervisory authority Integritetsskyddsmyndigheten (called Datainspektionen until 2021-01-01), prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within 48 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities,

with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the primary business contacts established on contract signing.

2. The data controller parties shall be under obligation to continuously to inform each other of changes to contacts/contact points.

3. The data controller may contact the data processor regarding
    any data processing related questions by using the following contact information:

    Kiona Holding AS
    Att: CTO
    Leirfossvegen 27, 7038 Trondheim, Norway
    Email us at: dataprotection@kiona.com
    Call us: +47 982 50 007

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

- Providing the data controller with a Proptech platform as a service for building system connectivity, building data analysis and energy optimization at the best possible quality and support level.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

- Authenticate and authorize the data controllers' users online for security reasons
- Build smart solutions to gain insights about the data controllers building portfolio performance
- Build smart machine learning based solutions that benefits the data controller
- Build smart steering algorithms, controlling the operations of the data controllers buildings with the purpose to reduce environmental impact, improve operation profit, employee satisfaction and tenant satisfaction
- Process data controller's order and manage data controllers accounts.
- Keep the data controller informed about service issues and maintenance
- Inform the data controller about updates to products, applications or services the data controller have purchased from Kiona.
- Invite the data controllers users to various events such as training, seminars, etc.
- Email the data controller with special offers on other products and services.
- Perform customer surveys such as NPS

The data processor also collect product usage statistics from the data controller users via Google Analytics (Kiona has signed DPA with Google) with the purpose of understanding how the products are used and from that analyse and gain insights on how to improve the product, services and customer support.

Specifically, identifiers such as the users

- UserId (not identifiable by third party)
- Customer identifier
- Google analytics cookies
- App instance IDs
- Anonymized IP addresses are used to measure user interactions with the data processors product modules and are shared with Google Analytics which is currently hosted in a third country (USA). IP addresses used to provide and protect the security of the service, and to give a sense of where in the world the users come from - are anonymized.

This information is also shared with our Microsoft Power BI platform (North Europe region) to

allow for the data processor to build internal reports to analyse and gain insights on how to improve the product, services and customer support. This data is not used to do any sort of user profiling, advertising or any other commercial purposes.

A personal consent regarding this is acquired from the data controllers users through our web interface for Kiona Edge.

The data processor receives and process data from Sensors and IOT equipment installed in the buildings and apartments that belongs to the data controller (like values for temperature, humidity, CO_2, VOC etc) on behalf of the data controller. This is a necessity to be able to deliver smart algorithms, validate controlling strategies, machine learning and historical data based multi-tenant cross customer values reflected in services available for the data controller as a customer. Please note that if a tenant in his agreement with the data controller "opt-out" from having a sensor installed in the tenant's apartment - that may compromise the quality of the product / services supplied by the data processor.

A.3. The processing includes the following types of personal data about data subjects:

- First and last name
- Title
- Phonenumber for your workplace and your mobile phone (work)
- Email Address (Work)
- Visiting address for your workplace
- Company Name
- Organization identifier
- Role in Kionas systems (Authorization)
- Apartment numbers
- Properties physical addresses
- Sensordata from apartments (Temperature, Humidity, CO_2, VOC etc)

A.4. Processing includes the following categories of data subject:

- Employees
- Suppliers
- Tenants

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

The data processor will keep the data controllers personal identification data as long as the data controller has a user accounts in the Kiona Edge platform. If the data controller terminates the contract with the data processor and stops the subscription, the accounts information will be deleted within a month.

Exceptions to the above is sensor data which will be kept but anonymized after contract termination- ensuring smart algorithms that are based on historical data still will be working as expected for all other customers.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	ADDRESS	DESCRIPTION OF PROCESSING
Microsoft	One Microsoft way, Redmond, Washington, 98052-6399 USA	Microsoft Power BI Reports
Google	1600 Amphitheatre Parkway, Mountain View, California, USA	Google analytics, usage statistics, Google cloud services

The data controller shall on the commencement of the Clauses authorise the use of the above-mentioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors

As described in 7.3

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

As described in Appendix A

C.2. Security of processing
The level of security shall take into account:

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

Personal data in the form of sensor values shall be encrypted all the way from when they are gathered in the sensor to the receiving cloud solution and be decrypted in the cloud.
When using the data processors own IOT infrastructure sensors communicate with Hubs and Gateways with Wireless M-bus traffic using strong encryption. These encrypted messages are then sent directly from the Gateways or Hubs to the data processors dedicated cloud platform (no intermediaries). The traffic between these communication devices that are connected in the telecom operator's network and the data processors cloud platform (Google cloud) uses encryption with certificates.
When the data controller is instructed to use third party IOT infrastructure the data controller should validate the security measures from that vendor and have a DPA signed with the third party vendor.

To prevent congestion attacks the data processors Hub's and Gateways uses filtering in the software. Only messages from accredited entities (Determined from the cloud service Edge) will be accepted all other messages are rejected immediately.
Configurations send to the data processors Hubs and Gateways are protected from attack or manipulation through the same encryption as mention above.
A Hub always connects to the data processors cloud solution. It is from there that it gets its "control data". Thus, you can only change how a Hub should behave, make a diagnosis, change the configuration, etc. if you are an administrator and are logged in to our cloud platform Edge -again hosted in Google cloud. You cannot connect to the data processors Hub and affect it directly.
The data processors Hub gets the DNS from the telecom operator who points out where our endpoint is. For a break attack to succeed, the attacker would have to hack the telecom operator and also crack the "double" encryption.
Update of Hubs and Gateways firmware is performed continuously OTA "over the air". An update OTA can only be initiated by the data processor and the software is downloaded from the data processors hosted environment in Google cloud. Secure verification / validation of the updated software is done automatically by the built-in module from Gemalto
https://www.gemalto.com/m2m/solutions/modules-terminals/industrial/ehs5

Backup of the services and data provided by the data processor is performed by Google cloud services making sure you get some of the best availability and recovery available.

The data processor performs yearly review of the processes involved in personal data processing.

To access data online users must login through the Edge web- interface which uses strong encryption.
Authentication happens via a separate Identity Server, Authorization of users managed by the data controllers registered administrators.
Original administration accounts are created by the data processors staff based on behalf of the data controller. After that more user accounts can be added by the data controller's administrator accounts.
User passwords must be at least 8 characters long and consist of a combination of small and big letters and numbers. The passwords are stored encrypted and when a password is reset passwords are never sent out through email.

All traffic to and from the data processors cloud platform (Google cloud) uses strong encryption with certificates and the same applies to all API traffic which also uses the OAuth2 security standard for authentication. This also applies to integrations made between the data processor and other systems – for instance when receiving sensor data from other vendors through API communications.

Edge is hosted in Google cloud and hence relies on data storage security and firewalls from the vendor. Currently the data is located in Google cloud region europe-west1 , see https://cloud.google.com/compute/docs/regions-zones/

The data processor solutions are behind firewalls and specifically for Kiona Edge it is behind Google cloud firewall.

For more information read https://cloud.google.com/security/
All logging is done to our cloud platform Edge (hosted in Google cloud) through our endpoint. The local diagnostic logs are also sent in this way.
For protective monitoring the data processor have automatic audit logs of all Edge events.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

Having processes ready for in a timely manner respond to the data controllers' rights.

Having a process for incident handling.

C.4. Storage period/erasure procedures

Personal data is stored according to A.5.

Upon termination of the provision of personal data processing services, the data processor shall delete the personal data in accordance with Clause 11.1., unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:
- EU/EES
- USA

C.6. Instruction on the transfer of personal data to third countries

As described in detail in A.2 the data processor collect usage statistics from the data controllers logged in users and how they use the data processor products via Google Analytics which are stored in USA. The purpose is to get an understanding how the products are used and from that analyse and gain insights on how to improve the product, services and customer support.

The transfer is protected by standard contractual clauses.

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data controller or the data controller's representative shall with at least one week prior notice perform a physical inspection of the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing to ascertain the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

In addition to the planned inspection, the data controller may perform an inspection of the data processor when the data controller deems it required. Prior to the inspection an NDA must be signed by the data controller.

The data controller's costs, if applicable, relating to physical inspection shall be defrayed by the data controller. The data processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

Appendix D The parties' terms of agreement on other subjects

This DPA is part of Kiona Edge General Terms and Conditions.

Appendix E Change log

VERSION #	CHANGED BY	CHANGE DATE	DESCRIPTION OF
1.5	Carl-Fredrik Bang	15.02.2023	Added Appendix E Change log to the document