

Standard Contractual Clauses

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

between

The “Buyer”, as defined in “General Terms and Conditions for Kiona” (GTC), **2. Definitions**,

(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	3
3. The rights and obligations of the data controller.....	3
4. The data processor acts according to instructions	4
5. Confidentiality	4
6. Security of processing	4
7. Use of sub-processors.....	5
8. Transfer of data to third countries or international organisations	6
9. Assistance to the data controller	7
10. Notification of personal data breach	8
11. Erasure and return of data.....	8
12. Audit and inspection	8
13. The parties' agreement on other terms	9
14. Commencement and termination	9
15. Data controller and data processor contacts/contact points.....	9
Appendix A Information about the processing	10
Appendix B Authorised sub-processors.....	14
Appendix C Instruction pertaining to the use of personal data	16
Appendix D The parties' terms of agreement on other subjects	20

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 Software as a Service, 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 State¹ 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 written 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 30 days 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, Datatilsynet (The Norwegian "Datatilsynet" will always be the competent supervisory authority, however, cooperation with other supervisory authorities where cross border cases are being addressed), 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, Datatilsynet, 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.

The data processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

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 following contacts/contact points:
2. The parties shall be under obligation 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 through the provided detail:

Name	Kiona Holding AS
Position	ATT: CTO
Telephone	+47 982 50 007
E-mail	dataprotection@kiona.com

Appendix A Information about the processing

Page 10 of 21

Kiona
Internal

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

Depending on the application(s) procured by the data controller;

1. Providing the data controller with building integration platform to help the data controller digitize, monitor, and control buildings in an open and flexible manner.
2. Providing the data controller with a PropTech platform as a service for building system connectivity, building data analysis and energy optimisation.
3. Providing the data controller with an Energy Management System (EMS) for energy, waste, and environmental reporting.

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):

Kiona
Internal

Nature of processing	Edge	Energinet	IWMAC	Web Port
Enabling data controller to extend the Energy Management System (EMS) with additional data and calculations.	x	✓	x	x
Enabling data controller to make data-driven decisions and remotely control buildings based on insights.	x	✓	✓	✓
Implement secure authentication and authorization for the data controller's users.	✓	✓	✓	✓
Develop steering algorithms and/or smart functions/ML to control the operations of data controller's buildings, aiming to reduce environmental impact, improve operational profit, and enhance employee and tenant satisfaction.	✓	x	✓	✓
Develop optimisation, reporting, and visualisation tools to benefit the data controller.	x	✓	✓	✓
Develop machine learning-based solutions that provide advantages to the data controller.	✓	x	x	x
Develop solutions, gaining insights into the data controller's building portfolio performance.	✓	x	x	x
Initiate advertising campaigns to showcase special offers on products and services.	✓	✓	✓	✓
Provide insights into the data controller's buildings.	x	x	✓	✓
Analyse and provide insights into the data controller's consumption of energy.	x	✓	x	x
Keep the data controller informed about updates to products, applications, or services purchased from Kiona.	✓	x	✓	✓
Extend invitations to various events, such as training sessions and seminars, to the data controller's users.	✓	✓	✓	✓
Maintain open communication with the data controller, keeping them informed about service issues and maintenance.	✓	✓	✓	✓
Conduct customer surveys, such as Net Promoter Score (NPS), to gather feedback.	✓	✓	✓	✓
Process data controller's orders and manage data controller's accounts.	✓	x	x	x
Send alarms and/or reports to the data controller's appropriate users.	x	✓	✓	✓
Share data with integrated systems configured by the data controller.	x	✓	✓	✓
Establish a robust mechanism for storing historical data for configured data points on behalf of the data controller.	x	✓	✓	✓
The data processor receives and processes data (such as values for temperature, humidity, CO2, VOC, etc.) from Controllers Sensors and IoT equipment, installed in the buildings and apartments that belong to the data controller on behalf of the data controller. This is essential to deliver effective building management functionality.	x	✓	✓	✓

Note: Where applicable (depending on solution), 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:Kiona
Internal

General Personal Data	Edge	Energinet	IWMAC	Web Port
Name (Fist & Surname)	✓	✓	✓	✓
Phone Mobile	✓	✓	✓	✓
Company Name/Firm	✓	✓	✓	✓
Visiting address (work)	✓	✓	✓	✗
Postal Address	✓	✗	✓	✗
Title/Position/Role	✓	✓	✓	✗
Phone Work (can also be a mobile)	✓	✓	✓	✗
Email (Work)	✓	✓	✓	✓
Department	✗	✓	✓	✗
Cost Centre/Payment Details	✓	✓	✓	✓
Organisation Identifier	✓	✗	✗	✗
Apartment Numbers	✓	✗	✗	✓
Properties Physical Address	✓	✓	✗	✓
Sensor data from apartment (Temperature, Humidity, CO2, VOC, etc)	✓	✓	✗	✓
Preferred Language	✗	✓	✓	✓
Role in Solution (Authorization)	✗	✓	✓	✓
Country	✓	✓	✓	✓
Expiry date (Account)	✗	✓	✗	✓
Location Data				
GPS	✗	✗	✓	✗
Wi-Fi Location data	✗	✗	✗	✗
Data processor/Customer network Location Data	✗	✗	✓	✗
IP-address	✗	✓	✗	✓
Data Traffic				
Personal data processed relating to maintaining electronic communication	✗	✗	✓	✗
Invoicing	✓	✗	✓	✗
Communications Data				
Emails	✓	✓	✓	✓
Telephone responses	✓	✓	✓	✓
SMS/MMS	✓	✓	✓	✓
Browser Data	✓	✓	✓	✓
Survey data (NPS)	✓	✓	✓	✓
Meeting Minutes	✓	✓	✓	✓
Logging				
Audit Log	✗	✓	✓	✓

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

Data Subjects	Edge	Energinet	IWMAC	Web Port
<i>Customers Employees</i>	✓	✓	✓	✓
<i>Kiona's Partners</i>	✗	✓	✓	✓
<i>Suppliers</i>	✓	✓	✓	✓
<i>Tenants</i>	✓	✓	✓	✓

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:

1. The data processor will keep the data controller's personal identifiable information data for as long as the data controller has active user accounts and subscriptions to any of data processors solutions. If the data controller terminates the contract with the data processor, and stops the subscription, the account(s) information will be deleted within a month.
2. Historical data is exempt, and the data processor reserves the right to keep said data in anonymized form after contract termination, to be used for continued development of solutions and in overall sustainability goals.

Appendix B Authorised sub-processors**Kiona
Internal****B.1. Approved sub-processors**

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

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING	KIONA PRODUCT
ATEA AS	976 239 997	Ranheimsvegen 9 N-7044 Trondheim Postboks 6288, Torgarden N-7489 Trondheim	Hosting services (Private cloud)	IWMAC
HubSpot Inc.	IE9849471F	2 nd Floor, 30 North Wall Quay, IFSC, Dublin 1	CRM System	ALL
Younium AB	559102-2875	c/o SUP46, Regeringsgatan 65, 111 65 Stockholm	Subscription management	ALL
Visma AS	936 796 702	Karenslyst Allé 56, 0277 Oslo, Norway	Subscription Invoicing	ALL
Microsoft		One Microsoft way, Redmond, WA 98052 - 6399 USA	• Microsoft Power BI * • Azure Cloud Services • MS365	EDGE * WebPort ALL
Google	IE3668997OH	1600 Amphitheatre Parkway, Mountain View, CA, 94043 USA	Google analytics 4	EDGE
Freshworks	33-1218825	2950 S. Delaware st, Suite 201, San Mateo, CA, 94403 USA	Freshdesk Support and Ticketing <i>Phased out by end year 2025.</i>	EDGE
Ahá		Menlo Park, San Francisco CA 94025 USA	Ticketing system	ALL
Zendesk		989 Market St. San Francisco, CA 94103 USA	Ticketing and support system	IWMAC Energinet
Nexthop	993821403	Drammensveien 288, 0283 Oslo	Private Cloud Hosting	Energinet

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:

Physical security

The data processor's cloud solutions (regardless of private or public cloud) are hosted on international and large-scale hosting suppliers in the Nordics or within EES Nations. This ensures that the solutions are available and scalable, while at the same time being monitored and kept up to date by competent third party suppliers with dedicated specialists within network and data security.

Supplier certifications:

Certification Standard	Azure	GCP	Private Cloud
ISO 9001 (Quality Management System)	Yes	Yes	Yes
ISO 14001 (Environmental Management System)	No	No	Yes
ISO 27001 (Information Security Management System)	Yes	Yes	Yes

For private cloud, ITIL management is applied.

Organisational security

The data processor's management model ensures that the solution is developed and maintained in a responsible manner. Data is managed in accordance with GDPR, which is contractually anchored with our customers through this DPA (Data Processing Agreement.)

Confidentiality

Data collected on behalf of our customers is temporarily stored on the gateway before it is sent to the cloud solution. Access to the system is only granted through registered users in the system. Users are limited to data from facilities where they are defined as users. Passwords are encrypted in the database. Access to configuration, requires MFA, and all changes to configuration and login is logged to the system.

Personal data, in the form of sensor values shall be encrypted from the point of collection and through transit to the cloud, where it will be decrypted for processing. (Edge/Webport)

Each data controller (customer) shall have their own isolated instance - containing historical data and independent from other customers.

Integrity

The transfer of data between the cloud solution and our application consumed by end users is protected with https (Certificates supplied by renowned CA's) as communication protocol.

Solutions that offer VPN as communication carrier (IWMAC) to secure data transferred between gateway from the customer's network to the cloud solution. The cloud solution uses authentication to ensure that the sender of the data is a valid gateway. For the IoT gateway, MQTTS with client certificate is used as the communication protocol with our cloud solution.

All web traffic to and from the data processors public cloud platforms (GCP & AZURE) uses strong encryption (typical TLS1.2 RSA-certs or stronger). The same applies to all API traffic, traffic between the data processor and other systems, for instance when receiving data from other vendors through API communication.

Availability

Private cloud hosted solution (IWMAC) is set up using two physically separated data centres. Data is written to an active-active storage solution across the two centres. The sites are connected using a high-speed communication and redundant network solution, in addition to redundant external networks. The network infrastructure of the datacentres benefits from 24/7 monitoring by the cloud provider. All components (Firewalls, Routers, and Switches) are secured with a High Availability (HA) cluster setup and are supplied by reputable suppliers. Configuration and monitoring are subject to a strict safety regime at the supplier and can only be performed by authorized personnel.

Public cloud hosted solutions rely on vendor specific robustness and preventive mechanisms to guarantee system and solution availability.

Analytical

The EDGE solution utilises Google Analytics V4 in combination with power BI. The processing involves only data that has been fully anonymised.

To read more about data privacy within Azure see:

<https://azure.microsoft.com/en-us/explore/trusted-cloud/privacy/>

For security related information around Azure hosted environments see:

<https://learn.microsoft.com/en-us/azure/security/fundamentals/>

To read more about data privacy within GCP see:

<https://cloud.google.com/privacy?hl=en>

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:

1. Having processes ready for in a timely manner respond to the data controllers' rights.
2. Having a process for incident handling.

C.4. Storage period/erasure procedures

“Personal data is stored for according to A.5 after which the personal data is erased by the data processor.

Upon termination of the provision of personal data processing services, the data processor shall either delete or return 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:

1. EU/EEC
2. USA (Edge only – fully anonymised data)

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

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 ONE MONTH 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”

“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.”

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

“The data processor or the data processor’s representative shall with at least ONE MONTH prior notice perform a physical inspection of the places, where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing to ascertain the sub-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 processor may perform an inspection of the sub-processor when the data processor (or the data controller) deems it required.

Documentation for such inspections shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new inspection under a revised scope and/or different methodology.

Based on the results of such an inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.”

Appendix D The parties' terms of agreement on other subjects

Page 20 of 21

**Kiona
Internal**

The DPA is part of the data processors General Terms and Conditions.

Appendix E Change Log**Kiona**

VERSION #	CHANGE BY	CHANGE DATE	DESCRIPTION OF CHANGE
1.2.0	CTO	15.02.2023	Added appendix E Changelog to the document.
1.9.0	ISM	08.03.2024	Merger of all Kiona products into one common DPA affecting all amendable sections of the document.
2.0.0	ISM	11.03.2024	Adjustments: A2 – Consolidation of items A3 – Corrections in coverage and formatting B1 – Completed org data
2.0.1	ISM	21.11.2024	Including Versioning in header
2.0.2	ISM	22.09.2025	Clarification of language of Nature of Processing. Labelling of EOL for authorised sub-processor.