APPENDIX I – DATA PROCESSING AGREEMENT

This APPENDIX I – DATA PROCESSING AGREEMENT including Sub-appendix 1 – Instructions for the Processing of Personal Data and Sub-appendix 2 – List of Approved Sub-processors (this "**DPA**") constitutes an appendix to and forms an integral part of the Verisure Business Customer General Terms and Conditions (the "**Main Contract**"), which applies when Verisure Services (UK) Limited ("**Verisure**" and the "**Data Processor**") processes personal data on behalf of the Business Customer ("**Data Controller**") when providing the Services and Equipment to the Data Controller via the alarm system.

The Data Processor and the Data Controller are hereinafter each referred to as a "**Party**" and jointly as the "**Parties**".

1 BACKGROUND

1.1 This DPA governs the rights and obligations of the Data Controller and the Data Processor when the Data Processor processes personal data on behalf of the Data Controller, pursuant to the Main Contract.

1.2 If the information stipulated in the Main Contract conflicts with this DPA, this DPA shall take precedence. In the event of any contradictions between this document and the Data Controller's documented instruction, this document shall take precedence, unless otherwise specifically stipulated or clearly indicated by the circumstances.

1.3 This DPA aims to meet the current requirements for a DPA in accordance with Applicable Data Protection Legislation.

1.4 This DPA shall remain in force for as long as the Data Processor processes personal data on the Data Controller's behalf. This DPA applies to and covers any changes, additions, or amendments to the Main Contract unless the Parties enter into a new data processing agreement. If the Main Contract is terminated and a new contract with a similar scope and purpose to the Main Contract is entered into between the Parties, while a new data processing agreement is not entered into, this DPA shall apply to the new Main Contract. This also applies if an explicit reference is made to this DPA in a contract between the Data Controller and Data Processor.

2 DEFINITIONS

Any capitalised terms utilised within this DPA, yet not expressly defined herein, shall carry the meaning ascribed to them in the Main Contract. The terms used in this DPA are defined in this section or directly in the sections where the terms are used. Where terms defined in the GDPR (as defined below) are used, those terms shall have the same meaning as in the GDPR, unless otherwise specified.

"Applicable Data Protection Legislation"	means all privacy, data protection and personal data laws of the United Kingdom, European Union ("**EU**") or a member state of the European Union applicable to the personal data processing that is carried out under this DPA.
"Business Customer"	means the customer named and a party to the Main Contract signed with Verisure.

“Data Controller”	has the meaning set forth in the recitals.
“Data Processor”	has the meaning set forth in the recitals.
“DPA”	has the meaning set forth in the recitals.
“Main Contract”	has the meaning set forth in the recitals.
"**Party**" and "**Parties”**	has the meaning set forth in the recitals.
“SCC”	means the standard contractual clauses for the transfer of personal data to data processors established in third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, implemented by the European Commission decision (EU) 2021/914 of 4 June 2021.
“Sub-processor”	means the legal person who is engaged by the Data Processor to carry out specific processing activities on behalf of the Data Controller.
“Sub-processor Notice”	has the meaning set forth in Section 8.2.
“UK”	means the United Kingdom.
“UK GDPR”	Regulation (EU) 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) (“**GDPR**”) as implemented in United Kingdom the Data Protection Act 2018.
“UK IDTA”	means the United Kingdom’s International Data Transfer Agreement or International data transfer addendum to the European Commission’s standard contractual clauses for international data transfers, as applicable and amended from time to time.

3 OBLIGATIONS OF THE DATA CONTROLLER

3.1 The Data Controller undertakes to ensure that there is a legal basis for the processing and for compiling correct instructions with regard to the nature of the processing so that

the Data Processor and any Sub-processor can fulfil their obligations according to this DPA and the Main Contract, where applicable.

3.2 The Data Controller shall, without undue delay, inform the Data Processor of changes in the processing which affect the Data Processor's obligations pursuant to Applicable Data Protection Legislation.

3.3 The Data Controller is responsible for informing data subjects, whose personal data is subject to processing under this DPA, about the processing and to safeguard the rights of data subjects in accordance with Applicable Data Protection Legislation, as well as to take every other measure required of the Data Controller pursuant to Applicable Data Protection Legislation.

4 PROCESSING OF PERSONAL DATA

4.1 The Data Processor shall ensure compliance with Applicable Data Protection Legislation as well as its obligations under this DPA when processing personal data on behalf of the Data Controller.

4.2 The Data Processor may only process personal data on behalf of the Data Controller in accordance with the Data Controller's documented instructions, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by the laws of the United Kingdom, European Union or a member state of the European Union to which the Data Processor is subject, in which case the Data Processor shall inform the Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.3 The Data Controller's initial instructions are set out in this DPA and Sub-appendix 1. Subsequent instructions may also be given by the Data Controller throughout the duration of the processing of personal data. These instructions shall always be documented.

4.4 The Data Processor shall immediately inform the Data Controller if, in its opinion, the Data Processor has not received sufficient instructions to process personal data in accordance with its obligations pursuant to the Main Contract or if, in the Data Processor's opinion, an instruction infringes Applicable Data Protection Legislation, and defer the processing until further instructions from the Data Controller are provided.

4.5 If the Data Controller persists with an instruction which, in the Data Processor's opinion, infringes Applicable Data Protection Legislation pursuant to Section 4.4, the Data Processor shall have the right to terminate the Main Contract, including this DPA, according to Section 14.3. In the event that the Data Processor has informed the Data Controller that an instruction may be potentially unlawful, the Data Processor shall in no way be held liable if it refuses to act on these instructions which are contrary to UK law, EU law or EU member state law or any other legal obligation of the Data Processor arising from UK law, EU law or EU member state law. If the Data Controller persists in the unlawful instruction, the Data Processor has the right to terminate the Main Contract between the Data Controller and the Data Processor with immediate effect. In any case, if the Data Processor has informed the Data Controller of the potentially unlawful nature of its instructions, the Data Processor shall not be held liable, directly or indirectly, for breaching any legislation, in the broadest sense and including any data protection legislation, for the execution of this instruction.

4.6 The Data Processor shall, without undue delay, inform the Data Controller about technical, organisational, or financial changes, including changes in the ownership, which

are likely to affect the Data Processor's capability of complying with its obligations in accordance with this DPA.

5 THE DATA PROCESSOR'S OBLIGATIONS TO ASSIST THE DATA CONTROLLER

5.1 The Data Processor shall assist the Data Controller in fulfilling its obligations in accordance with Applicable Data Protection Legislation per the Data Controllers request. This means that the Data Processor shall:

a) through appropriate technical and organisational measures, to the extent possible and with due regard to the nature of the processing, assist the Data Controller in fulfilling the Data Controller's obligations to respond to requests for exercising the data subjects right laid down in Chapter III of the UK GDPR (such as rectification, deletion, restriction, data portability and request of access);

b) assist the Data Controller in fulfilling the Data Controller's obligations to take appropriate security measures for the processing of personal data under this DPA to ensure a level of security appropriate considering the level of risk which the processing of personal data in question entails in accordance with Article 32 of the UK GDPR;

c) assist the Data Controller by providing the information, assistance and resources that are reasonably necessary for fulfilling the Data Controller's obligation to report personal data breaches to the competent supervisory authority in accordance with Article 33 of the UK GDPR;

d) assist the Data Controller with the information, assistance and resources that may reasonably be required to fulfil the Data Controller's obligation to inform the data subject, within the framework of this DPA, in the event of a data breach that is likely to result in a high risk to the rights and freedoms of natural persons in accordance with Article 34 of the UK GDPR;

e) assist the Data Controller in fulfilling the Data Controller's obligation to carry out data protection impact assessments for processing under this DPA, which is likely to result in a high risk to the rights and freedoms of individuals in accordance with Article 35 of the UK GDPR; and

f) assist the Data Controller by providing the Data Controller with the information, assistance and resources that may reasonably be required to fulfil the Data Controller's obligation to provide information and documentation to the supervisory authority for prior consultation, and when necessary, and to a reasonable extent, attend meetings with the supervisory authority in accordance with Article 36 of the UK GDPR.

5.2 When the Data Processor assists the Data Controller in fulfilling the Data Controller's obligations under Applicable Data Protection Legislation in accordance with Sections 5.1 b) – f) above, consideration shall be given to the type of processing it refers to, and the information available to the Data Processor. In order to avoid any misunderstandings, nothing in this section shall be interpreted as indicating that the Data Processor may act on behalf of the Data Controller. The Data Processor may only act to fulfil its obligations vis-à-vis the Data Controller.

6 SECURITY AND CONFIDENTIALITY

6.1 The Parties' obligations to observe confidentiality is regulated in the Main Contract. The Data Processor shall ensure that any Sub-processors that are engaged by the Data

Processor is subject to a confidentiality undertaking corresponding to the provisions under the Main Contract.

6.2 The Data Processor undertakes to take all appropriate technical and organisational measures to protect the personal data being processed under this DPA in accordance with Applicable Data Protection Legislation and in particular Article 32 of the UK GDPR. The Data Processor shall ensure that its service fulfils the requirements of the principles of privacy by design and privacy by default in line with Applicable Data Protection Legislation as set out in the Main Contract and this DPA.

6.3 The Data Processor has implemented the technical and organisational measures set out in the instructions from the Data Controller and undertakes not to substantially change these or otherwise change the security measures in a way that results in a lower level of security than the one intended in Section 6.2 and the Data Controller's instructions.

6.4 The Data Processor is obliged to immediately inform the Data Controller if the Data Processor considers that the implemented security measures no longer comply with the requirements set out in the Applicable Data Protection Legislation and wait for further instructions from the Data Controller.

6.5 The Data Processor shall ensure that only the personnel who must have access to the personal data in order to fulfil the Data Processor's obligations under this DPA will have access to such personal data. The Data Processor shall ensure that all such personnel are bound by appropriate confidentiality obligations, either by law or by agreement. The Data Processor shall also ensure that the personnel understand what confidentiality obligation entails.

7 PERSONAL DATA BREACHES

7.1 The Data Processor shall without undue delay after the Data Processor having become aware of the personal data breach, notify the Data Controller.

7.2 A notification pursuant to Section 7.1 shall include all information which may reasonably be required by the Data Controller to fulfil its obligations under Applicable Data Protection Legislation. Such information includes e.g. a description of:

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

b) the details of a contact point where more information concerning the personal data breach can be obtained;

c) likely consequences as a result of the data breach; and

d) the measures taken or proposed to be taken to rectify the personal data breach, including, where appropriate, measures to mitigate its potential adverse effects.

7.3 Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information available and further information shall, as it becomes available, subsequently be provided without undue delay.

7.4 The Data Controller shall compensate the Data Processor for any direct costs that the Data Processor incurs if the measures taken under this Section 7 are due to the Data Controller's non-compliance of Applicable Data Protection Legislation.

7.5 The Data Processor is not entitled to inform any third parties, including data subjects, of the personal data breach without the Data Controller's prior written consent, unless

required to do so by the laws of the United Kingdom, European Union or a member state of the European Union to which the Data Processor is subject.

8 SUB-PROCESSORS

8.1 The Data Processor is aware that it must comply with the requirements specified in Article 28(2) and (4) of the UK GDPR in order to engage a Sub-processor.

8.2 The Data Processor has the Data Controller's general written authorisation for the engagement of Sub-processors. The Data Processor shall inform the Data Controller in writing of any intended changes concerning the addition or replacement of Sub-processors ("**Sub-processor Notice**") at least thirty (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). A Sub-processor Notice to the Data Controller, to engage or replace a Sub-processor shall be in writing and as a minimum include the following information:

(i) company name;

(ii) company registration number (or equivalent);

(iii) address and country;

(iv) a description of the sub-processing; and

(v) where the personal data will be processed.

8.3 Should the Data Controller not approve an addition or replacement of a Sub-processor, the Data Controller has the right to terminate this DPA in accordance with Section 14.

8.4 A list of approved Sub-processors at the time of entering into this DPA is set forth in Sub-appendix 2. The Data Processor shall, from time to time, maintain an updated list of the Sub-processors who have been approved by the Data Controller, as well as the countries in which these Sub-processors perform their activities. At the Data Controller's request, the Data Processor shall submit a copy of the list to the Data Controller.

8.5 Where the Data Processor engages a Sub-processor for carrying out specific processing activities on behalf of the Data Controller, the Data Processor shall enter into an agreement with the Sub-processor which imposes corresponding obligations as are applicable to the Data Processor in accordance with this DPA, and under which the Sub-processor also provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this DPA and Applicable Data Protection Legislation. 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 this DPA and Applicable Data Protection Legislation.

8.6 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 this DPA 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.

8.7 If the Sub-processor does not fulfil their 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.

9 DATA TO A THIRD COUNTRY

9.1 The Data Processor may transfer personal data on behalf of the Data Controller to a third country or an international organisation, provided such transfers meet the requirements and undertakings which follow from Applicable Data Protection Legislation and the Data Controller's instructions. The Data Processor undertakes to enter into the UK IDTA and, where applicable, the relevant module of the SCCs with its Sub-processors that transfer personal data to a third country or an international organisation, unless another applicable transfer mechanism applies, and to take all reasonable measures to control that the engaged Sub-processors ensure the lawfulness of any further transfers of personal data that the Sub-processors' sub-processors may undertake.

9.2 The Data Processor shall inform the Data Controller, without undue delay, if an adequate level of protection can no longer be guaranteed for the transfer of personal data to, or access from, a third country or an international organisation or if the transfer or processing can, in any other way, be considered contrary to the Applicable Data Protection Legislation. Furthermore, in such instances, the Data Processor shall immediately take steps to ensure that personal data can continue to be processed in accordance with Applicable Data Protection Legislation and inform the Data Controller of the measures taken.

10 REQUEST FOR INFORMATION AND DISCLOSURE OF PERSONAL INFORMATION

10.1 In cases where a data subject or other third party requests information from the Data Processor in respect of processing of personal data which belongs to the Data Controller, the Data Processor shall refer such data subject or third party to the Data Controller.

10.2 In the event a public authority requests the type of data as set forth in Section 10.1 above, the Data Processor shall immediately inform the Data Controller of the request, unless prevented by law, and the Data Processor and the Data Controller shall, in consultation, agree on a suitable course of action.

10.3 The Data Processor shall not disclose or make any personal data which belongs to the Data Controller available unless the Data Processor is under legal obligation deriving UK law or from EU member state or European Union law, or court or public authorities' order to disclose the information (provided that such court or public authority is located within the United Kingdom or European Union).

10.4 If an obligation to disclose information as stipulated in Section 10.3 above emerges, the Data Processor shall immediately inform the Data Controller of such situation if not prohibited by law.

11 AUDIT AND DOCUMENTATION

11.1 The Data Processor shall make available to the Data Controller all information necessary to demonstrate that the Data Processor has fulfilled its obligations in accordance with this DPA and Applicable Data Protection Legislation. At the Data Controller's request, the Data Processor shall also permit and contribute to audits of the processing activities covered by this DPA, at reasonable intervals or if there are indications of non-compliance. The Data Controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the Data Processor. The Data Controller shall ensure that such independent third party is subject to confidentiality.

11.2 The Data Processor shall, at all times, be entitled to reasonable notice in the event the Data Controller wishes to exercise its right to conduct an audit.

11.3 If an audit pursuant to this Section 11 indicates that the Data Processor has breached its obligations under this DPA or Applicable Data Protection Legislation, the Data Processor shall, without undue delay, remedy such deficiency.

12 LIABILITY

12.1 Subject to the limitation of liability set out in the Main Contract, if the Data Processor processes personal data in violation of this DPA or Applicable Data Protection Legislation, the Data Processor shall compensate the Data Controller for the damage caused by the Data Processor due to the incorrect processing.

12.2 In the event of compensation for damages in connection with wrongful processing of personal data, which, through an established judgment or settlement, shall be payable to the data subject due to a breach of the provisions in this DPA, the Data Controller's instructions and/or Applicable Data Protection Legislation, Article 82 of the UK GDPR shall apply.

12.3 This liability claim, as set out in this Section 12 of the DPA, takes precedence over any liability claim in the Main Contract with regards to processing of personal data.

12.4 The Parties' liability for compensation in accordance with this Section 12 will apply even if the DPA is terminated or otherwise cease to apply.

13 CONTRACT PERIOD

With the exception of Sections 6 and 12, the provisions of this DPA shall apply for as long as the Data Processor processes personal data on the Data Controller's behalf.

14 EARLY TERMINATION

14.1 The Data Processor shall immediately inform the Data Controller if the Data Processor, for whatever reason, is unable to fulfill its obligations under this DPA.

14.2 If the Data Processor is not able to remedy and fulfil its obligations under this DPA prior to thirty (30) days after having informed the Data Controller pursuant to Section 14.1, the Data Controller shall have the right to terminate the Main Contract and this DPA.

14.3 For termination of this DPA pursuant to Section 4.5, the termination provisions of the Main Contract shall apply.

15 MEASURES IN CONNECTION WITH THE TERMINATION

15.1 When this DPA expires, the Data Processor shall, at the Data Controller's request and per the Data Controllers instructions, permanently delete, or return in a format that the Data Controller chooses, all personal data processed in accordance with the DPA to the Data Controller and delete all existing copies, unless the Data Processor is required by Union or Member State law to save a copy of the personal data.

15.2 In this context, deletion means that the personal data is deleted in accordance with the industry standard in force at any given time in order to make it impossible for the data to be recreated using technology or method known at the time of deletion. This shall also apply to personal data that has been processed for logging and security purposes.

16 AMENDMENTS

16.1 If Applicable Data Protection Legislation changes during the term of this DPA, or if competent supervisory authority issues guidelines, decisions or regulations concerning the application of Applicable Data Protection Legislation that result in this DPA no longer meeting the requirements for a data processing agreement, this DPA shall be changed

in order to meet such new or additional requirements. The Parties shall mutually and in writing agree on such changes.

16.2 The Data Processor shall, without undue delay and for a reasonable fee, implement additional security measures upon the Data Controller's requests.

16.3 Other amendments and additions to the DPA shall, in order to be binding, be in writing and duly signed by both Parties. If the Main Contract specifies a process for amendments to the agreement, this shall also be applicable in regard to amendments to this DPA.

17 DISPUTE SETTLEMENT AND APPLICABLE LAW

What is stipulated in the Main Contract applies to dispute settlement and choice of law.

SUB-APPENDIX 1 – INSTRUCTIONS FOR THE PROCESSING OF PERSONAL DATA

The following document is the Data Controller's instructions to the Data Processor.

Definitions used in this instruction shall have the same meaning as in the DPA, unless circumstances clearly indicate otherwise.

1 PROCESSING OF PERSONAL DATA

1.1 Purpose of processing.

In order to enable the use and allow for User Content as part of Verisure's services, Verisure will process personal data by transmitting it from the Equipment to the App and/or user account.

1.2 Subject-matter of the processing.

The subject-matter of the processing is the provision of Verisure's Services, which include the use and the possibility to create User Content.

1.3 Categories of personal data.

Depending on the Services and Equipment that the Data Controller have chosen, Verisure shall collect and process the following categories of personal data:

a) livestream;

b) still pictures;

c) video recordings; and

d) audio recordings.

1.4 Categories of data subjects.

The content collected by the Data Controller's active use of the Services entail that Verisure shall process the personal data of those individuals present in the protected property.

1.5 Processing activities (nature of the processing).

The use and User Content include functionalities such as:

a) live view streaming;

b) continuous video recording;

c) recording of video, photo or audio;

d) video doorbell; and

e) smart door lock.

1.6 Transfer to third countries.

Verisure does not currently transfer data to third countries. Verisure stores personal data in the European Economic Area ("**EEA**") or in countries with an appropriate level of data protection. These countries have data protection laws equivalent to those of the United Kingdom. If Verisure discloses personal data to companies established outside (i) the EEA or (ii) countries with an appropriate level of data protection, Verisure contractually requires these companies to process personal data on similar terms as those stated in this DPA. In such situations, Verisure will ensure that the personal data transferred is

protected. Upon request, Verisure can provide further information regarding such transfers where applicable.

1.7 Duration.

As stated in the Main Contract.

2 TECHNICAL AND ORGANISATIONAL SECURITY MEASURES.

Cybersecurity is a key topic for Verisure, and Verisure is continuously investing in advancing this function and ensuring that Verisure adapt to the evolving threats landscape. Verisure's commitment to cybersecurity means constantly staying ahead of emerging risks and vulnerabilities. Through rigorous monitoring, encryption, penetration testing, stringent access control, employee awareness and continuous improvement of Verisure's systems, Verisure strive to strengthen its defences against data breaches. Upon request, Verisure can provide further information regarding any transfer.

SUB-APPENDIX 2 – LIST OF APPROVED SUB-PROCESSORS

Definitions used in this list of approved Sub-processors shall have the same meaning as in the DPA, unless circumstances clearly indicate otherwise.

Verisure is entitled to engage the following Sub-processors for the processing of personal data within the scope of this DPA.

Name of Sub-processor	**Company registration address**	**Description of the sub-processing**	**Location for the processing of personal data (country)**
Amazon Web Services EMEA SARL trading as AWS	38 Avenue John F. Kennedy, L-1855 Luxembourg.	Cloud storage, cloud computing	European Economic Area
Microsoft Iberica S.R.L. providers of Microsoft Azure	Microsoft Iberica S.R.L. Paseo Del Club Deportivo 1, Centro Empresarial La Finca, Edificio 1. 28223 Pozuelo de Alarcón, Madrid. Spain. VAT Number: ESB78603495	Cloud storage, cloud computing	European Economic Area
Oracle Ibérica, S.R.L. providers of Oracle Cloud	Oracle Ibérica, S.R.L. Paseo de la Castellana, 81 28046 Madrid (Madrid), España NIF: B-78361482. Reg. Merc. Madrid Tomo 9629, Folio 28, Hoja M-51948	Cloud storage	European Economic Area
Verisure Arlo Europe DAC	Verisure Arlo Europe DAC, Building 4100 Cork Airport Business Park, Cork, Ireland, T12 AP97.	Cloud Storage for Orion and Aquilla cameras or Arlo cameras through Verisure subscription.	European Economic Area

APPENDIX II – JOINT CONTROLLER ARRANGEMENT

This APPENDIX II – JOINT CONTROLLER ARRANGEMENT (this "**Joint Controller Arrangement**") constitutes an appendix to and forms an integral part of the Verisure Business Customer General Terms and Conditions (referred herein as the "**Main Contract**"), which applies when Verisure Services (UK) limited ("**Verisure**") provides Services and Equipment to Business Customers via the System.

Verisure and the Business Customer are hereinafter each referred to as a "**Party**" and jointly as the "**Parties**".

1 BACKGROUND

1.1 The Parties have entered into the Main Contract which includes the provision of Verisure's Service(s) to the Business Customer. Under the Service(s), the Parties will process certain personal data for purposes and means jointly decided by the Parties, as further described in Section 3.

1.2 The purpose of this Joint Controller Arrangement is to document the Parties' arrangement on the allocation of the Parties' respective responsibilities in a contract for compliance with the obligations under the UK GDPR when acting as joint controllers. However, if the Business Customer is subject to the household and personal data exemption in the UK GDPR as explained in section 14.4 of the Main Contract, Verisure will be the sole data controller and this Joint Controller Arrangement does not apply.

2 DEFINITIONS

2.1 The terms in this Joint Controller Arrangement shall have the same definition attributed to them as in the Main Contract if not expressly defined herein.

2.2 In addition, the terms in this Joint Controller Arrangement shall be interpreted in accordance with the **GDPR**, unless otherwise specified.

3 JOINT CONTROLLERS

3.1 This Joint Controller Arrangement sets out the respective obligations of the Parties relating to the joint processing of personal data under the Service(s).

3.2 **Purpose**. The purpose(s) of the processing is to (i) monitor the premises through the Service(s) in order to ensure the safety and security of the Business Customer and other individuals by enabling the Service(s), and (ii) to share personal data in the forms of live view streaming, CVR, recording of video, photos or audio of an incident directly with the Business Customer through the My Verisure App in order to manage and follow up an alarm signal.

3.3 **Subject matter**. The Verisure Equipment, such as the control panel, movement detector, voice panel, cameras, fire alarm, etc., collect personal data passively and continuously as well as when the Service is activated by sending signals to Verisure in order to allow for the triggering of a Security Signal when necessary. In case the collected signals trigger an alarm event, the alarm event is queued to Verisure's ARC and Verisure's Equipment begin collecting personal data in the forms of images and audio. Depending on the Business Customer's choice of Verisure Equipment, the collected personal data may also be shared directly with the Business Customer through the My Verisure App.

3.4 The Parties agree that they shall be considered joint controllers for the processing of personal data regarding the collection and intake of personal data from Verisure's Equipment for the provision of the ARC Alarm Management Service as well as when Verisure shares the personal data directly with the Customer through the My Verisure App in order to manage and follow up an alarm signal.

3.5 **Categories of personal data**. The processing includes personal data in the form of signals from Verisure's Equipment, such as alarm logs, as well as, in case of an alarm event, images, video and audio that may include personal data if the data subject is present when the alarm is triggered. When personal data is collected by sending signals to Verisure, no personal data in the form of images or audio is collected by the Verisure's Equipment.

3.6 **Categories of data subjects**. The categories of data subjects include individuals present in the monitored area.

4 OVERALL DISTRIBUTION OF RESPONSIBILITIES

4.1 Each Party shall fulfil its own regulatory obligations under the UK GDPR, unless otherwise specified in this Joint Controller Arrangement.

4.2 The Business Customer shall ensure that it complies with any legal obligations regarding alarm monitoring.

5 GENERAL DATA PROTECTION PRINCIPLES AND LEGAL BASIS FOR THE PROCESSING

5.1 The Parties are separately responsible for complying with the principles of processing personal data as set out in Article 5 of the UK GDPR.

5.2 The Parties may not process personal data under this Joint Controller Arrangement for any other purpose than the purpose jointly defined by the Parties, unless required to do so by UK, European Union or EU Member State law to which the Party is subject. For the avoidance of doubt, this does not limit the Business Customer's use of personal data for Convenience use and/or User content.

5.3 Notwithstanding the foregoing, Verisure may further process the personal data for the subsequent purposes set out in Verisure's Privacy Notices relating to the processing of personal data for the provision of the Services and other related legitimate processing purposes. The Business Customer may further process personal data for its own purposes to protect its own interests such as to provide the personal data to its insurance company, to the police authority or to other governmental authorities in criminal or civil proceedings within the United Kingdom.

5.4 The legal basis for the processing by Verisure shall be its legitimate interest. The Business Customer is responsible for ensuring that it has a legal basis for the processing of personal data and that the legal basis is documented.

6 RIGHTS OF DATA SUBJECTS

According to the UK GPDR, the data subjects have a number of rights in relation to the Parties, including:

- information obligation when collecting personal data from the data subject (Article 13);
- information obligation when personal data have not been collected by the data subject (Article 14);

- right of access by the data subject (Article 15);
- right to rectification (Article 16);
- right to erasure ("right to be forgotten") (Article 17);
- right to restriction of processing (Article 18);
- notification obligation regarding rectification or erasure of personal data or restriction of processing (Article 19);
- right to data portability (Article 20); and
- right to object (Article 21).

7 DISTRIBUTION OF RESPONSIBILITIES

7.1 The Parties are responsible for assisting each other to the extent that this is relevant and necessary for them to comply with the obligations towards the data subjects.

7.2 The Business Customer shall inform the data subjects about the joint processing of personal data and Verisure's subsequent processing of personal data by referring the data subjects to Verisure's Privacy Notice for Business Customer's data subjects, available at www.verisure.co.uk/privacy-page#business-visitor.

7.3 Verisure is responsible for handling data subject requests regarding the rights as set out in Section 6. Both Parties are responsible for ensuring that it is completely clear to the data subjects that Verisure serves as the point of contact for the exercise of the data subject rights.

7.4 Irrespective of the content of the arrangement as set out in this section, the data subject may contact either of the Parties to exercise his or her rights in accordance with Article 26(3) of the UK GDPR.

8 SECURITY MEASURES

8.1 The Parties are responsible for complying with Article 32 of the UK GDPR concerning security of processing. This means that each Party shall take appropriate technical and organisational measures to ensure a level of security proportionate to the risk, taking into account the current technical level, the implementation costs and the nature, extent, coherence and purpose of the processing concerned, as well as the risks of varying probability and seriousness of the rights and freedoms of natural persons.

8.2 Each Party shall comply with the requirement to ensure privacy by design and privacy by default under Article 25 of the UK GDPR.

9 DATA PROCESSORS AND SUB-PROCESSORS

9.1 Verisure is entitled to use data processors and sub-processors in connection with the joint processing under this Joint Controller Arrangement. In such case, Verisure shall comply with the requirements under Article 28 of the UK GDPR.

9.2 Verisure shall inform the Business Customer, upon request, of whether the personal data is processed by data processors and, if relevant, sub-processors.

10 DATA PROCESSING RECORDS

Each Party shall be obliged to maintain a record of processing activities in compliance with Article 30 of the UK GDPR.

11 NOTIFICATION OF PERSONAL DATA BREACHES

11.1 The Parties are responsible to observe Article 33 of the UK GDPR concerning notification of a personal data breach, relating to the processing under this Joint Controller Arrangement, to the supervisory authority. Upon becoming aware of such personal data breach, the Party affected by the personal data breach shall notify the other Party without undue delay. The Party affected by the personal data breach shall then, in consultation with the other Party, take the necessary measures to fulfil the requirements under Article 33 of the UK GDPR. The Parties are responsible for assisting each other to the extent that this is relevant and necessary for the Party affected by the personal data breach to comply with the obligations under Article 33 of the UK GDPR.

11.2 The Business Customer is responsible to communicate a notification of a personal data breach, relating to the processing under this Joint Controller Arrangement, to the data subjects in accordance with Article 34 of the UK GDPR. Verisure is responsible for assisting the Business Customer to the extent that this is relevant and necessary for the Business Customer to comply with the obligations under Article 34 of the UK GDPR.

12 DATA PROTECTION IMPACT ASSESSMENTS

12.1 The Parties are responsible to observe the requirements in Article 35 of the UK GDPR concerning data protection impact assessments. This means, that the Parties, where a type of processing, in particular using new technologies and taking in to account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data or to document that such an assessment is not necessary.

12.2 The Parties are responsible to observe the requirement in Article 36 of the UK GDPR concerning prior consultation with the supervisory authority, when appropriate, and shall consult with each other prior to any contact with the supervisory authority.

13 THIRD COUNTRY TRANSFERS

The Parties have jointly agreed that Verisure may decide to transfer personal data to third countries. In such case, Verisure is responsible to observe the requirements of Chapter 5 in the UK GDPR.

14 CONTACT AND AVAILABILITY

Verisure acts as the point of contact for data subjects in relation to this Joint Controller Arrangement.

15 INFORMATION TO THE OTHER PARTIES

The Parties shall inform each other about significant matters that affect the joint processing and this Joint Controller Arrangement.

16 ENTRY INTO FORCE AND TERMINATION

This Joint Controller Arrangement is valid for the duration of the joint processing of the personal data under the Joint Controller Arrangement.

17 LIABILITY AND CONFLICT

Each Party shall indemnify and hold the other Party harmless from all claims, sanctions, damages, expenses (including reasonable attorney's fees) and direct losses arising out of or relating to any failure by that Party and its employees, agents, subcontractors or a

person or company authorised by that Party to process personal data to comply with the provisions of this Joint Controller Arrangement.

18 APPLICABLE LAWS AND DISPUTE RESOLUTION

The provisions regarding applicable laws and dispute resolution in the Main Contract apply also to this Joint Controller Arrangement.

19 MISCELLANEOUS

This Joint Controller Arrangement constitute an integral part of the Main Contract. In case of any conflict between this Joint Controller Arrangement and the Main Contract, the Joint Controller Arrangement shall prevail between the Parties to the extent of such conflict or inconsistency.