Data Protection Policy

Please note this document is intended to be read in conjunction with the Webeye Service level agreement, SIM contract and general terms and conditions of sale with which it co-exists.

This Policy sets out how We process the personal data that we hold. It outlines our responsibilities under data protection legislation and regulation, setting out how it will comply, and provides instruction for staff handling personal data.

The Policy applies to **all** members of staff

1. Introduction

We believe that the protection of individuals via the lawful, legitimate and responsible processing and use of their personal data is a fundamental human right. Individuals may have a varying degree of understanding or concern for the protection of their personal data, but it is imperative that Webeye respects their right to have control over their personal data and ensure it acts in full compliance with legislative and regulatory requirements at all times. If individuals feel that they can trust Webeye as a custodian of their personal data, this will also help Webeye to fulfil its wider objectives.

2. Scope

As aforementioned, these requirements and objectives apply to **all** members of Staff employed by Webeye, including if applicable, contractors, or interns who are carrying out work on behalf of Webeye involving the handling personal data. We impress upon all members of staff that they have a crucial role to play in ensuring that Webeye maintains the trust and confidence of the individuals about whom Webeye processes personal data (including its own staff), complying with webeye's legal obligations and protecting Webeye's reputation. Compliance with this Policy and the related legislation and British Standards and the procedures based thereon is mandatory. Any breach of this Policy and any related policies and procedures may result in disciplinary action.

All members of staff, across all services divisions, must understand and comply with this Policy when processing personal data in the course of performing their tasks and must observe and comply with all controls, practices, protocols and training to ensure such compliance.

The Data Protection and Privacy Officer is responsible for overseeing the implementation and review of this Policy (and the related policies and procedures). They can be contacted at **data-protection@webeyecms.com**

If you do not feel confident in your knowledge or understanding of this Policy, or you have concerns regarding the implementation of this Policy, it is important that you raise this issue with your line manager as soon as possible or use the contact details above to seek advice.

3. Legislation

The main piece of legislation that governs how Webeye collects and processes personal data is The General Data Protection Regulation (GDPR), as supplemented by the Data Protection Act DPA 2018 (DPA), in conjunction with **BS50518 which is a British standard produced by the British standards institute and specifically governs regulation surrounding all aspects of the alarm receiving centre protocols** including the capture, storage and use of alarm, video and associated personal data for both its own staff and that of all third party stakeholders using the service. By conforming to those standards, Webeye has to comply with certain stringent data storage and Cyber security requirements used within a central station environment. All

data is held on AWS and tier 3/4 collocated data centres and **complies with ISO27001**. Webeye is also a member of the **BSIA**.

Compliance with British Standards and the procedures based thereon is mandatory. Any breach of this Policy and any related policies and procedures may result in disciplinary action.

BS50518 is a British standard produced by the British standards institute and governs regulation surrounding all aspects of the **Alarm Receiving Centre Protocols**. This Standard applies to all Monitoring and Alarm Receiving Centres (MARC's) that monitor and/or receive and/or process signals that require an emergency response. The BS EN 50518 series of standards apply to alarm signals generated from intruder and hold-up alarm systems (I&HAS) only. Alarm signals from other types of alarm systems, i.e. fire, social and closed circuit television systems (CCTV) are not within the scope of the BS EN 50518 series.

In addition all clients utilizing the Webeye portal will have accepted the terms of our SLA, which includes among its provision the following section:

6.2 The Service Provider shall be responsible for ensuring that it complies with all statutes, regulations, byelaws, standards, codes of conduct and any other rules relevant to the provision of the Services.

Accordingly given that the platform is predicated on the basis of being compliant with **BS50518**, these are the now well documented procedures to which we consistently adhere, and we are unable to depart from the same save in exceptional circumstances; given that to do so, we feel, would create a completely ad hoc arrangement entirely contrary to **BS50518**; we believe that consistency of policy will benefit everyone involved and ensure compliance with British Standards.

4. Data Protection Principles

Under these alarm receiving standards **BSEN 50518** (parts 1 to 3) requires that **NSI Gold Alarm Receiving Centres**, (which is the standard to which we adhere) keep such data for at least 2 years for compliance purposes; in particular Webeye's Records Management and Retention Policy (developed in accordance with BS50518) requires that:

1. All client data shall be retained for a minimum period of two years.
2. All data of ARC external communications shall be retained for a minimum period of three months.
3. A log of operator actions shall be retained for a minimum period of two years.
4. In addition Webeye must observe and comply with at all times from the moment that personal data is collected, until the moment that personal data are archived, deleted or destroyed that all personal data is
    a. Processed lawfully, fairly and in a transparent manner
    b. Collected only for specified, explicit and legitimate purposes
    c. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed (Data minimisation)
    d. Accurate and where necessary kept up to date.
    e. Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed.

f. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. Security, integrity and confidentiality is ensured via designated stringent data storage and Cyber security requirements used within a central station environment. As aforementioned all of our data is held on AWS and tier 3/4 collocated data centres and complies with ISO27001.
g. Webeye allows data subjects to exercise their rights in relation to their personal data subject to our overriding obligation under BS50518
h. Webeye is responsible for, and must be able to demonstrate compliance with, all of the above principles.

5. Further advice regarding this Policy

The Data Protection and Privacy Officer, or other relevant local contacts, can be contacted for general advice and if you:

- wish to process personal data for any purpose and you are unsure whether the Webeye has a lawful basis for doing so (see Lawfulness and fairness)
- need to rely on consent and/or require explicit consent (see Consent as a lawful basis for processing)
- need to prepare a fair processing notice (see Transparency)
- are unsure whether to delete, destroy or keep any personal data (see Storage limitation)
- are unsure about what security or other measures you need to take to protect personal data (see Security, integrity and confidentiality)
- know or suspect that there has been a personal data breach (see Reporting personal data breaches)
- are unsure on what basis to transfer personal data outside of the United Kingdom) (see Transfers outside the UK)
- if you need assistance in dealing with the exercise of any rights by data subjects (see Data subject rights and requests)
- if you plan to use personal data for any purposes other than those they were originally collected for (see Purpose limitation)
- if you are considering the processing of personal data in a new or different way, where a Data Protection Impact Assessment may be necessary (see Accountability and record-keeping)
- if you plan to undertake any activities involving automated processing including profiling or automated decision-making
- if you are unsure of the legal requirements relating to any direct marketing activities (see Direct marketing)
- if you need help with contracts or any other areas in relation to sharing personal data with a third party (see Sharing personal data).

6. Lawfulness, fairness and transparency

6.1 Lawfulness and fairness

In order to collect and process personal data for any specific purpose, Webeye must always have a lawful basis for doing so. Without a lawful basis for processing, such processing will be unlawful and unfair and may also have an adverse impact on the affected data subjects. No data subject should be surprised to learn that their personal data has been collected, consulted, used or otherwise processed by Webeye. Processing personal data will only be lawful where at least one of the following lawful bases applies:

6.1.1 The data subject has given their **consent** for one or more specific purposes

6.1.2 The processing is necessary for the **performance of a contract** to which the data subject is a party (for instance a contract of employment or registration with Webeye)

6.1.3 To comply with Webeye's **legal obligations**

6.1.4 To protect the **vital interests** of the data subject or another person (this will equate to a situation where the processing is necessary to protect the individual's life)

6.1.5 To pursue Webeye's **legitimate interests** where those interests are not outweighed by the interests and rights of data subjects (only available to the company in some circumstances)

6.1.6 Webeye must identify and document the lawful basis relied upon by it in relation to the processing of personal data for each specific purpose or group of related purposes.

6.2 Consent as a lawful basis for processing

There is no hierarchy between the lawful bases for processing above, of which a data subject's consent is only one. Consent may not be the most appropriate lawful basis depending on the circumstances.

In order for a data subject's consent to be valid and provide a lawful basis for processing, it must be:

6.2.1 specific (not given in respect of multiple unrelated purposes)

6.2.2 informed (explained in plain and accessible language)

6.2.3 unambiguous and given by a clear affirmative action (meaning opt-in: silence, inactivity or pre-ticked boxes will not be sufficient)

6.2.4 separate and unbundled from any other terms and conditions provided to the data subject

6.2.5 freely and genuinely given (there must not be any imbalance in the relationship between Webeye and the data subject and consent must not be a condition for the provision of any product or service)

6.2.6 A data subject must be able to withdraw their consent as easily as they gave it.

6.2.7 Once consent has been given, it will need to be updated where Webeye wishes to process the personal data for a new purpose that is not compatible with the original purpose for which they were collected.

6.2.8 Unless Webeye is able to rely on another lawful basis for processing, a higher standard of explicit consent (where there can be no doubt that consent has been obtained, for example a signed document or a Yes/No option accompanied by clear consent wording) will usually be required to process special categories of personal data, for automated decision-making and for transferring personal data outside of the United Kingdom.

6.2.9 Where Webeye needs to process special categories of personal data, it will generally rely on another lawful basis that does not require explicit consent; however, Webeye must provide the data subject with a fair processing notice explaining such processing.

6.2.10 If Webeye is unable to demonstrate that it has obtained consent in accordance with the above requirements, it will not be able to rely upon such consent.

6.3 Transparency

6.3.1 The concept of transparency runs throughout the GDPR and requires Webeye to ensure that any information provided by Webeye to data subjects about how their personal data will be processed is concise, easily accessible, easy to understand and written in plain language. Where Webeye has not been transparent about how it processes personal data, this will call the lawfulness and fairness of the processing into question.

6.3.2 Webeye can demonstrate transparency through providing data subjects with appropriate privacy notices or fair processing notices **before** it collects and processes their personal data and at appropriate times throughout the processing of their personal data.

6.3.4 The GDPR sets out a detailed list of information that must be contained in all privacy notices and fair processing notices, including the types of personal data collected; the purposes for which they will be processed; the lawful basis relied upon for such processing (in the case of legitimate interests, Webeye must explain what those interests are); the period for which they will be retained; who Webeye may share the personal data with; and, if Webeye intends to transfer personal data outside of the UK, the mechanism relied upon for such transfer (see Transfers of personal data outside of the UK).

6.3.5 Where Webeye obtains any personal data about a data subject from a third party it must check that it was collected by the third party in accordance with the GDPR's requirements and on a lawful basis where the sharing of the personal data with Webeye was clearly explained to the data subject.

6.3.6 All privacy notices and fair processing notices should be reviewed by the the Data Protection and Privacy Officer (data-protection@Webeyecms.com)

7. Purpose limitation

7.1 Webeye must only collect and process personal data for specified, explicit and legitimate purposes that have been communicated to data subjects **before** the personal data have been collected.

7.2 Webeye must ensure that it does not process any personal data obtained for one or more specific purposes for a new purpose that is not compatible with the original purpose. Where Webeye intends to do so, it must inform the data subjects **before** using their personal data for the new purpose and, where the lawful basis relied upon for the original purpose was consent, obtain such consent again.

8. Data minimisation

8.1 The personal data that Webeye collects and processes must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed.

8.2 You must only process personal data when necessary for the performance of your duties and tasks and not for any other purposes. Accessing personal data that you are not authorised to access, or that you have no reason to access, may result in disciplinary action and in certain circumstances, may constitute a criminal offence.

8.3 You may only collect personal data as required for the performance of your duties and tasks and should not ask a data subject to provide more personal data than is strictly necessary for the intended purposes.

8.4 You must ensure that when personal data are no longer needed for the specific purposes for which they were collected, that such personal data are deleted, destroyed or anonymised.

8.5 You must observe and comply with Webeye's Records Management and Retention Policy adhering to BS50518 which governs regulation surrounding all aspects of the alarm receiving centre protocols namely

8.5.1 **All client data shall be retained for a minimum period of two years.**

8.5.2 **All data of ARC external communications shall be retained for a minimum period of three months.**

8.5.3 **A log of operator actions shall be retained for a minimum period of two years.**

9. Accuracy

9.1 The personal data that Webeye collects and processes must be accurate and, where necessary, kept up-to-date and must be corrected or deleted without delay when Webeye discovers, or is notified, that the data are inaccurate.

9.2 You must ensure that you update all relevant records if you become aware that any personal data are inaccurate. Where applicable, any inaccurate or out-of-date records should be deleted or destroyed.

10. Storage limitation

10.1 The personal data that Webeye collects and processes must not be kept in a form that identifies a data subject for longer than is necessary in relation to the purposes for which it was collected of the express requirements of **BS50518**.

10.2 Storing personal data for longer than necessary may increase the severity of a data breach and may also lead to increased costs associated with such storage.

10.3 Webeye will maintain policies and procedures to ensure that personal data are deleted, destroyed or anonymised in accordance with **BS50518** .

10.4 You must regularly review any personal data processed by you in the performance of your duties and tasks to assess whether the purposes for which the data were collected have expired and requirements of **BS50518 require** that you must take all reasonable steps to delete or destroy any personal data that Webeye no longer requires in accordance with the Webeye's Records Management Policy as aforesaid.

10.5 All privacy notices and fair processing notices must inform data subjects of the period for which their personal data will be stored as defined by **BS50518**.

10.6 **You must observe and comply with Webeye's Records Management and Retention Policy which stipulates**

- **All client data shall be retained for a minimum period of two years.**
- **All data of ARC external communications shall be retained for a minimum period of three months.**
- **A log of operator actions shall be retained for a minimum period of two years.**

11. Data

Attention is drawn to the GDPR and BS50518.

11.1 General

The following categories of data are required:

11.1.1 client data

11.1.2 data of ARC external communications

11.1.3 log of operator actions

11.2 Client data

The data for each alarm system connected to the ARC shall be available to operators and shall include:

11.2.1 name, address and telephone contact number(s) of supervised premises;

11.2.2 premises reference number and any special arrangements;

11.2.3 name, address and telephone(s) numbers of users;

11.2.4 actions to be taken when an alarm occurs;

11.2.5 agreed setting and un-setting times where appropriate.

11.3 Data of ARC external communications

The data for each alarm system connected to the ARC shall be available to operators and shall include:

11.3.1 All data of external communications shall be recorded in a retrievable format.

11.3.2 A log shall be maintained recording the actions of the operator(s).

11.3.3 The log shall contain details of all the routine testing, maintenance and emergency servicing to ARC equipment.

12. Data storage

12.1 As aforementioned Webeye's Records Management and Retention Policy developed **expressly** in accordance with **BS50518** which governs regulation surrounding all aspects of the alarm receiving centre protocols stipulates

12.1.1 All client data shall be retained for a minimum period of two years.

12.1.2 All data of ARC external communications shall be retained for a minimum period of three months.

12.1.3 A log of operator actions shall be retained for a minimum period of two years.

13. Security, integrity and confidentiality

13.1 Security of personal data

13.1.1 Webeye's extensive auditing and password protected access of all stakeholders provides greater protection and unparalleled accountability should any breach of GDPR take place.

13.1.2 Webeye will ensure that all personal data that Webeye collects and processes must be secured by appropriate technical and organisational measures against accidental loss, destruction or damage, and against unauthorised or unlawful processing.

13.1.3 Webeye will continue to develop, implement and maintain appropriate technical and organisational measures for the processing of personal data taking into account the:

13.1.3.1 nature, scope, context and purposes for such processing
13.1.3.2 volume of personal data processed
13.1.3.3 likelihood and severity of the risks of such processing for the rights of data subjects
13.1.3.4 Webeye will regularly evaluate and test the effectiveness of such measures to ensure that they are adequate and effective.
13.1.3.5 You are responsible for ensuring the security of the personal data processed by you in the performance of your duties and tasks. You must ensure that you follow all procedures that Webeye has put in place to maintain the security of personal data from collection to destruction.
13.1.3.6 You must ensure that the confidentiality, integrity and availability of personal data are maintained at all times:
13.1.3.7 **Confidentiality:** means that only people who need to know and are authorised to process any personal data can access it
13.1.3.8 **Integrity:** means that personal data must be accurate and suitable for the intended purposes
13.1.3.9 **Availability:** means that those who need to access the personal data for authorised purposes are able to do so

13.1.4 You must ensure that you observe and comply with our Information security Policy which is again developed in accordance with BS50518.

13.1.5 You must not attempt to circumvent any administrative, physical or technical measures Webeye has implemented as doing so may result in disciplinary action and in certain circumstances, may constitute a criminal offence.

13. 2 Reporting personal data breaches

13.2.1 In certain circumstances, the GDPR will require Webeye to notify the ICO, and potentially data subjects, of any personal data breach.

13.2.2 Webeye has put in place appropriate procedures to deal with any personal data breach and will notify the ICO and/or data subjects where Webeye is legally required to do so.

13.2.3 If you know or suspect that a personal data breach has occurred, you must contact the the Data Protection and Privacy Officer, and IT Services if relevant, immediately to report it and obtain advice, and take all appropriate steps to preserve evidence relating to the breach.

13.2.4 You must ensure that you observe and comply with Webeye's personal data breach procedure.

14. Sharing personal data

14.1 You are not permitted to share personal data with third parties unless Webeye has agreed to this in advance, this has been communicated to the data subject in a privacy notice or fair processing notice beforehand and, where such third party is processing the personal data on our behalf, Webeye has undertaken appropriate due diligence of such processor and entered into an agreement with the processor that complies with the GDPR's requirements for such agreements.

14.2 The transfer of any personal data to an unauthorised third party would constitute a breach of the Lawfulness, fairness and transparency principle and, where caused by a security breach, would constitute a personal data breach. Do not share any personal data with third parties, including the use of freely available online and cloud services for work-related purposes, unless you are certain that the conditions outlined above apply. Seek advice from the **Data Protection and Privacy Officer** , or IT Services, if you are unsure.

15. Transfers outside of the United Kingdom

15.1 The GDPR prohibited the transfer of personal data outside of the EEA in most circumstances in order to ensure that personal data are not transferred to a country that does not provide the same level of protection for the rights of data subjects. In this context, a "transfer" of personal data includes transmitting, sending, viewing or accessing personal data in or to a different country. Restricted transfers from the UK to other countries , including to the EEA, are now subject to transfer rules under the UK regime.

15.1.1 These UK transfer rules broadly mirror the EU GDPR rules, but the UK has the independence to keep the framework under review.

15.2. The UK GDPR primarily applies to controllers and processors located in the United Kingdom, with some exceptions.

15.3 Individuals risk losing the protection of the UK GDPR if their personal data is transferred outside of the UK.

15.4 On that basis, the UK GDPR restricts transfers of personal data outside the UK, or the protection of the UK GDPR, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies.

15.5 A transfer of personal data outside the protection of the UK GDPR (which we refer to as a 'restricted transfer'), most often involves a transfer from the UK to another country.

Webeye may only transfer personal data outside of the UK in accordance with the following Checklist

15.6 Checklist

15.6.1 **Question 1. Are we planning to make a restricted transfer of personal data outside of the UK?** You are making a restricted transfer if: the UK GDPR applies to your processing of the personal data you are transferring.

If no, you can make the transfer. If yes go to Q2

15.6.2 **Question 2. Do we need to make a restricted transfer of personal data in order to meet our purposes?**

15.6.2.1 Before making a restricted transfer you should consider whether you can achieve your aims without actually sending personal data.

15.6.2.2 If you make the data anonymous so that it is never possible to identify individuals (even when combined with other information which is available to receiver), it is not personal data. This means that the restrictions do not apply and you are free to transfer the anonymised data outside the UK.

If no, you can make the transfer without any personal data. If yes go to Q3

15.6.3 **Question 3.Are there UK 'adequacy regulations' in relation to the country or territory where the receiver is located or a sector which covers the receiver** (which currently includes countries in the EEA and countries, territories or sectors covered by existing EU 'adequacy decisions')?

15.6.3.1 **What countries or territories are covered by adequacy regulations?**

15.6.3.1.1 The UK has "adequacy regulations" in relation to the following countries and territories:

- The European Economic Area (EEA) countries.
- These are the EU member states and the EFTA States.
- The EU member states are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.
- The EFTA states are Iceland, Norway and Liechtenstein.
- EU or EEA institutions, bodies, offices or agencies.
- Gibraltar.
- Countries, territories and sectors covered by the European Commission's adequacy decisions (in force at 31 December 2020)
- These include a full finding of adequacy about the following countries and territories:
- Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.
- In addition, the partial findings of adequacy about:
    - Japan – only covers private sector organisations.
    - Canada - only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA. For more details please see the EU Commission's FAQs on the adequacy finding on the Canadian PIPEDA.

If adequacy regulations are satisfied, you can make the transfer. If no go to Q4

15.6.4 **Question 4. Are we putting in place an 'appropriate safeguard' referred to in the UK GDPR?**

15.6.4.1 If there are no UK 'adequacy regulations' about the country, territory or sector for your restricted transfer, you should then find out whether you can make the transfer subject to 'appropriate safeguards'.
15.6.4.2 There is a list of appropriate safeguards in the UK GDPR. Each ensures that both you and the receiver of the restricted transfer are legally required to protect individuals' rights and freedoms in respect of their personal data.

If yes, go to Q5 If no go to Q6

15.6.5 **Question 5. Having undertaken a risk assessment, we are satisfied that the data subjects of the transferred data continue to have a level of protection essentially equivalent to that under the UK data protection regime.**

15.6.5.1 Before you may rely on an appropriate safeguard to make a restricted transfer, you must be satisfied that the data subjects of the transferred data continue to have a level of protection essentially equivalent to that under the UK data protection regime.
15.6.5.2 You should do this by undertaking a risk assessment, which takes into account the protections contained in that appropriate safeguard and the legal framework of the destination country (including laws governing public authority access to the data).
15.6.5.3 If your assessment is that the appropriate safeguard does not provide the required level of protection, you may include additional measures.

If yes, you can make the transfer. If no, go to Q6.

15.6.6 **Question 6 Does an exception provided for in the UK GDPR apply?**

15,6.6.1 Has the individual given his or her explicit consent to the restricted transfer?

15.6.6.2 Do you have a contract with the individual? Is the restricted transfer necessary for you to perform that contract? Are you about to enter into a contract with the individual? Is the restricted transfer necessary for you to take steps requested by the individual in order to enter into that contract.

15.6.6.3 Do you have (or are you entering into) a contract with an individual which benefits another individual whose data is being transferred? Is that transfer necessary for you to either enter into that contract or perform that contract?

15.6.6.4 You need to make the restricted transfer for important reasons of public interest.

15.6.6.5 You need to make the restricted transfer to establish if you have a legal claim, to make a legal claim or to defend a legal claim.

15.6.6.6 You need to make the restricted transfer to protect the vital interests of an individual. He or she must be physically or legally incapable of giving consent.

15.6.6.7 You are making the restricted transfer from a public register.

15.6.6.8 You are making a one-off restricted transfer and it is in your compelling legitimate interests.

15.6.6.8.1 If you cannot rely on any of the other exceptions, there is one final exception to consider. This exception should not be relied on lightly and never routinely as it is only for truly exceptional circumstances.

15.6.6.8.2 For this exception to apply to your restricted transfer:

15.6.6.8.2.1 there must be no UK 'adequacy regulations' which apply.

15.6.6.8.2.2 you are unable to use any of the other appropriate safeguards. You must give serious consideration to this, even if it would involve significant investment from you.

15.6.6.8.2.3 none of the other exceptions apply. Again, you must give serious consideration to the other exceptions. It may be that you can obtain explicit consent with some effort or investment.

15.6.6.8.2.4 your transfer must not be repetitive – that is it may happen more than once but not regularly.

15.6.6.8.2.5 the personal data must only relate to a limited number of individuals. There is no absolute threshold for this. The number of individuals involved should be part of the balancing exercise you must undertake in para (g) below.

15.6.6.8.2.6 The transfer must be necessary for your compelling legitimate interests. Please see the section of the guide on legitimate interests as a lawful basis for processing, but bearing mind that this exception requires a higher standard, as it must be a compelling legitimate interest. An example is a transfer of personal data to protect a company's IT systems from serious immediate harm.

15.6.6.8.2.7 On balance your compelling legitimate interests outweigh the rights and freedoms of the individuals.

15.6.6.8.2.8 You have made a full assessment of the circumstances surrounding the transfer and provided suitable safeguards to protect the personal data. Suitable safeguards might be strict confidentiality agreements, a requirement for data to be deleted soon after transfer, technical controls to prevent the use of the data for other purposes, or sending pseudo-anonymised or encrypted data. This must be recorded in full in your documentation of your processing activities.

15.6.6.8.2.9 You have informed the ICO of the transfer. We will ask to see full details of all the steps you have taken as set out above.

15.6.6.8.2.10 You have informed the individual of the transfer and explained your compelling legitimate interest to them.

If yes, you can make the transfer. If no, you cannot make the transfer in accordance with the UK GDPR.

15.7 if you reach the end without finding a provision which permits the restricted transfer, you will be unable to make that restricted transfer in accordance with the UK GDPR.

16. Data subject rights and requests

16.1 The GDPR provides data subjects with a number of rights in relation to their personal data. These include:

16.1.1 **Right to withdraw consent:** where the lawful basis relied upon by Webeye is the data subject's consent, the right to withdraw such consent at any time without having to explain why

16.1.2 **Right to be informed:** the right to be provided with certain information about how we collect and process the data subject's personal data (see Transparency)

16.1.3 **Right of subject access:** the right to receive a copy of the personal data that we hold, including certain information about how Webeye has processed the data subject's personal data

16.1.4 **Right to rectification:** the right to have inaccurate personal data corrected or incomplete dated completed.

16.1.5 **Right to erasure (right to be forgotten):** the right to ask Webeye to delete or destroy the data subject's personal data if: the personal data are no longer necessary in relation to the purposes for which they were collected; the data subject has withdrawn their consent (where relevant); the data subject has objected to the processing; the processing was unlawful; the personal data have to be deleted to comply with a legal obligation under BS50518; the personal data were collected from a data subject under the age of 13, and they have reached the age of 13.

16.1.6 **Right to restrict processing:** the right to ask Webeye to restrict processing if: the data subject believes the personal data are inaccurate; the processing was unlawful and the data subject prefers restriction of processing over erasure; the personal data are no longer necessary in relation to the purposes for which they were collected but they are required to establish, exercise or defend a legal claim; the data subject has objected to the processing pending confirmation of whether Webeye's legitimate interests grounds for processing override those of the data subject.

16.1.7 **Right to data portability:** in limited circumstances, the right to receive or ask Webeye to transfer to a third party, a copy of the data subject's personal data in a structured, commonly-used machine-readable format

16.1.8 **Right to object:** the right to object to processing where the lawful basis for processing communicated to the data subject was Webeye's legitimate interests and the data subject contests those interests.

16.1.9 **Right to object to direct marketing:** the right to request that we do not process the data subject's personal data for direct marketing purposes

16.1.9 **Right to object to decisions based solely on automated processing (including profiling):** the right to object to decisions creating legal effects or significantly affecting the data subject which were made solely by automated means, including profiling, and the right to request human intervention

16.1.10 **Right to be notified of a personal data breach:** the right to be notified of a personal data breach which is likely to result in a high risk to the data subject's rights or freedoms

16.1.11 **Right to complain:** the right to make a complaint to the ICO or another appropriate supervisory authority

16.2 You must be able to identify when a request has been made and must verify the identity of the individual making a request before complying with it. You should be wary of third parties deceiving you into providing personal data relating to a data subject without their authorisation.

16.3 You must immediately forward any request made by a data subject (even if you are uncertain whether it represents a request as set out above) to the **Data Protection and Privacy Officer**. Webeye will only have 30 days to respond in most circumstances.

16.4 You must observe and comply with Webeye's data subject access requests procedures from time to time.

17. Accountability and record-keeping

17.1 Webeye is responsible for and must be able to demonstrate compliance with the data protection principles and Webeye's other obligations under the GDPR and **BS50518**. This is known as the 'accountability principle'.

17.2 Webeye must ensure that it has adequate resources, systems and processes in place to demonstrate compliance with Webeye's obligations including:

17.2.1 appointing a suitably qualified and experienced Data Protection Officer (DPO) and providing them with adequate support and resource

17.2.2 ensuring that at the time of deciding how Webeye will process personal data, and throughout its processing, implementing appropriate technical and organisational measures that are designed to ensure compliance with the data protection principles and specifically **BS50518** which governs regulation surrounding all aspects of the alarm receiving centre protocols (known as 'Data Protection by Design')

17.2.3 ensuring that, by default, only personal data that are necessary for each specific purpose are processed both in relation to the nature, extent and volume of such personal data, the period of storage and the accessibility of the personal data (known as 'Data Protection by Default')

17.2.4 ensuring that where any intended processing presents a high risk to the rights and freedoms of data subjects, Webeye has carried out an assessment of those risks and is taking steps to mitigate those risks, by undertaking a '**Data Protection Impact Assessment**' (see below)

17.2.5 integrating data protection into Webeye's internal documents, privacy policies and fair processing notices

17.2.6 regularly training Webeye's staff on the **GDPR and BS50518** and, this policy and Webeye's related policies and procedures based thereon as aforesaid, and maintaining a record of training completion by members of staff

17.2.7 regularly testing the measures implemented by Webeye and conducting periodic reviews to assess the adequacy and effectiveness of this policy, and Webeye's Related policies and procedures

17.2.8 Webeye must keep full and accurate records of all its processing activities in accordance with the GDPR's and **BS50518** requirements.

17.2.9 You must ensure that you have undertaken the necessary training providing by Webeye and, where you are responsible for other members of staff, that they have done so.

17.2.10 You must further review all the systems and processes under your control to ensure that they are adequate and effective for the purposes of facilitating compliance with Webeye's obligations under this policy.

17.2.11 You must ensure that you observe and comply with all policies and guidance which form the Webeye's Information Governance Framework.

18. Data Protection Impact Assessments

18.1 A Data Protection Impact Assessment (DPIA), also known as a Privacy Impact Assessment, is a process to help identify and minimise the data protection risks involved in projects, processes and activities involving the processing of personal data. DPIAs are required for processing likely to result in high risk to the individuals and their personal data, and where new technologies are involved. In practice, Webeye requires a DPIA for any projects involving the use of personal data, including new systems, solutions and some research studies.

18.2 A DPIA must:

18.2.1 Describe the nature, scope, context and purposes of the processing

18.2.2 assess necessity, proportionality and compliance measures

18.2.3 identify and assess risks to individuals

18.2.4 identify any additional measures to mitigate those risks.

18.2.5 DPIAs need to be assessed and signed off by the Data Protection Officer and, where relevant, IT Services. Webeye's Data Protection Impact Assessment Policy provides full details and a template for conducting a DPIA.

19. Marketing and keeping You informed

19.1 to keep You informed about Our services, developments, pricing tariffs, special offers, and any discounts or awards which We believe may be of personal interest to You, or which You may be entitled to. We may keep You up to date directly to Your Phone, and by post, telephone and by voice, audio and videomail subject to any preferences indicated by You. You can contact Us at any time to ask Us not to use Your location or "communications data" for marketing purposes or if You would prefer not to receive direct marketing information, or simply to update Your preferences by writing to or calling Us, by sending an email to **sales@webeyecms.com**; (iii) to tell You about the products and special promotions of carefully selected partners (subject to Your preferences) and allow You to receive advertising and marketing information from them but without passing control of Your information to the third party concerned. You can update Your preferences at any time as described above.

19.2 to carry out market research.

19.3 to carry out activities necessary to the running of Our business, including system testing, network monitoring, staff training, quality control and any legal proceedings; and

19.4 to carry out any activities or disclosures to comply with any regulatory, government or legal requirement.

19.5 We may share Your information with other members of Our group of companies, and with Our, or their, partners, associates, agents and contractors who provide services to Us, and for the purposes of pursuing Our legitimate interests, including people who are interested in buying Our business. These may include people and companies outside the UK

19.6 We may also use data processors, some of whom may be based outside the UK, to process data on Our behalf and who provide specific services to Us and Our group of companies. If We do this, We will ensure that Your information is processed to the same standards adopted by Us;

19.7 If You use Our Services from a country outside the UK it may be necessary to transfer Your information to that country. In such circumstances the treatment of Your personal information may be subject to laws and

regulations applying in that country and which may not protect Your information to the same standards applying in the UK.

19.8 We will retain Your information for as long as is necessary in accordance with **BS50518** currently a minimum period of 2 years. Your account information will be kept after Your relationship with Us ends to comply with these legal and regulatory obligations.

You must keep any passwords and PIN numbers relating to Your Account and the Mobile Services safe and secure. You must not share them with anyone else. If You find or suspect that anyone else knows Your passwords or PIN numbers, or can guess them, You must contact Us immediately and ask Us to change them. **This is Your responsibility.**

19.9 You have the right to obtain a copy of personal data which We may hold about You. Please write to the **Data Protection and Privacy Officer, Innovation House, Kestral Road, Mansfield Nottinghamshire NG18 5FT** Alternatively, email: **services@webeyecms.com** . We may ask You to provide proof of Your identity and residence and may charge £10 to cover Our administrative costs.

If You have any questions about this notice or the way in which Your information is processed, please contact the Data Protection and Privacy Officer, by writing or sending an email to the above addresses. If We change this notice We will post the amended version on Our website so You always know how We will collect, use and disclose Your information. See www.webeyecms.com

20. Changes to this policy

20.1 Webeye may make amendments to this policy from time to time without notice, so please ensure you view the latest version.