Our Business is Protecting Yours

GDPRDOC1.0 Data Protection Policy Statement (Tier 1)

Contents

1. Introduction

AlertSystems Group Limited is committed to conducting its business in accordance with all applicable laws and regulations in respect of Personal Data, and the protection of the "rights and freedoms" of individuals whose information AlertSystems Group Limited collects and processes in accordance with the General Data Protection Regulation (GDPR).

This policy sets forth the expected behaviours of AlertSystems Group Limited's Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and deletion of any Personal Data belonging to an AlertSystems Group Limited customer (i.e. the Data Subject).

Personal Data is any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data. An organisation that handles Personal Data and makes decisions about its use is known as a Data Controller. AlertSystems Group Limited, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose AlertSystems Group Limited to complaints, regulatory action, fines and/or reputational damage.

AlertSystems Group Limited's Top Management is fully committed to ensuring continued and effective implementation of this policy, and expects all AlertSystems Group Limited's Employees and Third Parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

This policy has been approved by AlertSystems Group Limited's Board.

2. Scope

This policy applies to all AlertSystems Group Limited Companies where a Data Subject's Personal Data is processed:

- in the context of the business activities of AlertSystems Group Limited
- for the provision or offer of goods or services to individuals (including those provided or offered free-of-charge) by AlertSystems Group Limited

This policy applies to all processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

This policy has been designed to establish a standard for the processing and protection of Personal Data by all AlertSystems Group Companies. Where national law imposes a requirement which is stricter than imposed by this policy, the requirements in national law must be followed. Furthermore, where national law imposes a requirement that is not addressed in this policy, the relevant national law must be adhered to.

3. Definitions

Employee	An individual who works part-time or full-time for AlertSystems Group Limited under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. Includes temporary employees and independent contractors.
Third Party	External organisations with which an AlertSystems Group Limited company conducts business and is also authorised to, under the direct authority of AlertSystems Group Limited, process the Personal Data of AlertSystems Group Limited contacts.
Personal Data	Any information related to a natural person or 'Data Subject' that can be used to directly or indirectly identify the person.
Customer	Any past, current or prospective AlertSystems Group Limited customer.
Identifiable Natural Person	Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Controller	A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
Data Subject	A natural person whose personal data is processed by a controller or processor.
Process, Processing	Any operation performed on Personal Data, whether or not by automated means, including collection, use, storing, making available, deletion etc.
Data Protection	The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction.
Data Protection Authority	An independent Public Authority responsible for monitoring the application of the relevant Data Protection regulation set forth in national law. (Information Commissioner's Office).
Data Processors	The entity that processes data on behalf of the data controller.
Consent	Freely given, specific, informed and explicit consent of the Data Subject by statement or action signifying agreement to the processing of their personal data.
Special Categories of Data	Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.
Third Country	Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.

Personal Data Breach	A breach of security leading to the accidental or unlawful access to destruction, misuse, loss, alteration, unauthorised disclosure of Personal Data.
Encryption	Personal data that is protected through technological measures to ensure that the data is only accessible / readable by those with specified access.
Pseudonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without the use of additional data.
Anonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

4. Policy

4.1 Governance

4.1.1 Data Protection Team

To demonstrate our commitment to Data Protection, and to enhance the effectiveness of our compliance efforts, AlertSystems Group Limited has established a Data Protection Team. The Team operates with independence and is staffed by suitability skilled individuals granted all necessary authority. The Team reports to AlertSystems Group Limited's Compliance Manager, as appointed Data Protection Officer, who has direct access to the Board of Directors. The Data Protection Team's duties include:

- Informing and advising AlertSystems Group Limited and those employees who carry out processing of personal data of all laws and regulations applicable to Data Protection;
- Ensuring the alignment of this policy with Data Protection regulations and national law;
- Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);
- Acting as a point of contact for and cooperating with the Data Protection Authority (DPA);
- Determining the need for notifications to the DPA as a result of AlertSystems Group Limited's current or intended Personal Data processing activities;
- Making and keeping current notifications to the DPA as a result of AlertSystems Group Limited's current or intended Personal Data processing activities;
- The establishment and operation of a system providing prompt and appropriate responses to Data Subject requests;
- Informing Top Management and senior managers of AlertSystems Group Limited of any potential corporate, civil and criminal penalties which may be levied against AlertSystems Group Limited and/or its employees for violation of applicable Data Protection laws.
- Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any Third Party who:
    - provides Personal Data to AlertSystems Group Limited
    - receives Personal Data from AlertSystems Group Limited
    - has access to Personal Data collected or processed by AlertSystems Group Limited.

4.1.2 Policy Dissemination & Enforcement

The Data Protection Team shall ensure that all AlertSystems Group Limited employees and third parties responsible for the processing of Personal Data are aware of and comply with the contents of this policy. Assurance of such compliance shall be obtained from all third parties, whether companies or individuals, prior to granting them access to Personal Data controlled by AlertSystems Group Limited.

4.1.3 Data Protection by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them shall go through an approval process before continuing.

The Data Protection Team shall ensure that a Data Protection Impact Assessment (DPIA) is conducted for all new and/or revised systems or processes for which it has responsibility. Where applicable, the IT department shall cooperate with the Data Protection Team to assess the impact of any new technology uses on the security of Personal Data.

4.1.4 Compliance Monitoring

To confirm that an adequate level of compliance is being achieved by AlertSystems Group Limited in relation to this policy, the Data Protection Team shall undertake annual Data Protection compliance audits. Each audit will, as a minimum, assess:

- Compliance with Policy in relation to the protection of Personal Data, including:
  - The assignment of responsibilities.
  - Raising awareness.
  - Training of Employees.
- The effectiveness of Data Protection related operational practices, including:
  - Data Subject rights.
  - Personal Data transfers.
  - Personal Data incident management.
  - Personal Data complaints handling.
- The level of understanding of Data Protection policies and Privacy Notices.
- The currency of Data Protection policies and Privacy Notices.
- The accuracy of Personal Data being stored.
- The conformity of Data Processor activities.
- The adequacy of procedures for redressing poor compliance and Personal Data breaches.

The Data Protection Team shall devise a plan with a schedule for correcting any identified deviations within a defined and reasonable time frame. Any major deviations identified will be reported to and monitored by Top Management.

4.2 Data Protection Principles

All processing of personal data shall be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. AlertSystems Group Limited policies and procedures are designed to ensure compliance with the principles.

- Principle 1: Lawfulness, Fairness and Transparency
  Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, AlertSystems Group Limited shall tell the Data Subject what processing will occur (transparency), the processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

- Principle 2: Purpose Limitation
  Personal Data shall only be collected for specified, explicit and legitimate purposes and processed in a manner that is compatible with those purposes. This means AlertSystems Group Limited shall specify exactly what the Personal Data collected will be used for and limit the processing of that Personal Data to only what is necessary to meet the specified purpose.

- Principle 3: Data Minimisation
  Personal Data shall be adequate, relevant and limited to what is necessary for processing. This means AlertSystems Group Limited shall not store any Personal Data other than what is strictly required.

- Principle 4: Accuracy
  Personal Data shall be accurate and kept up to date with every effort to erase or rectify without delay. This means AlertSystems Group Limited shall have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

- Principle 5: Storage Limitation
  Personal Data shall be kept in a form such that the Data Subject can be identified only as long as is necessary for processing. This means AlertSystems Group Limited shall, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

- Principle 6: Integrity & Confidentiality
  Personal Data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, and possible damage and loss caused to individuals. AlertSystems Group Limited shall use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

- Principle 7: Accountability
  The Data Controller shall be responsible for, and be able to demonstrate compliance. This means AlertSystems Group Limited must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

4.3 Data Collection

4.3.1 Data Sources

Personal Data shall not be collected from the Data Subject unless one of the following applies:

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

If Personal Data is collected from someone other than the Data Subject, the Data Subject shall be informed of the collection unless one of the following applies:

- The Data Subject has received the required information by other means
- The information must remain confidential due to a professional secrecy obligation
- A national law expressly provides for the collection, processing or transfer of the Personal Data.

Where it has been determined that notification to a Data Subject is required, notification shall occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal Data
- At the time of first communication if used for communication with the Data Subject
- At the time of disclosure if disclosed to another recipient.

4.3.2 Data Subject Consent

AlertSystems Group Limited understands ‘consent’ to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the Data Subject’s wishes by statement or by a clear affirmative action signify agreement to the processing of personal data relating to him or her. The Data Subject can withdraw their consent at any time.

AlertSystems Group Limited shall obtain Personal Data only by lawful and fair means and, where appropriate, with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their Personal Data, AlertSystems Group Limited is committed to seeking such consent.

In most instances, consent to process personal and sensitive data is obtained routinely by AlertSystems Group Limited using standard consent documents; e.g. via contract documentation.

The Data Protection Team shall establish a system for obtaining and documenting Data Subject consent for the collection, processing, and/or transfer of their Personal Data. The system shall include provisions for:

- Determining what disclosures should be made in order to obtain valid consent
- Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
- Ensuring the consent is freely given (i.e. is not based on a contract that is conditional to the processing of Personal Data that is unnecessary for the performance of that contract).
- Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the consents given.
- Providing a simple method for a Data Subject to withdraw their consent at any time.

4.3.3 Data Subject Notification

AlertSystems Group Limited shall, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the processing of their Personal Data.

When the Data Subject is asked to give consent to the processing of Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The Data Subject already has the information
- A legal exemption applies to the requirements for disclosure and/or consent.

The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Compliance Manager. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

4.3.4 External Privacy Notices

Our website www.alertsystems.co.uk includes an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law. All Privacy and Cookie Notices shall be approved by the Group IT Manager and Compliance Manager prior to publication on any AlertSystems Group Limited external website.

4.4 Data Use

4.4.1 Data Processing

AlertSystems Group Limited uses the Personal Data of its customers for the following broad purposes:

- The general running and business administration of AlertSystems Group Limited
- To provide services to AlertSystems Group Limited customers.
- The ongoing administration and management of customer services.

The use of a customer's information shall always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be a customer expectation that their details will be used by AlertSystems Group Limited to respond to a request for information about products and services on offer. However, the customer would also reasonably expect that AlertSystems Group Limited would not then provide their details to Third Parties for marketing purposes.

AlertSystems Group Limited shall process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, AlertSystems Group Limited shall not process Personal Data unless at least one of the following requirements is met:

- The Data Subject has given consent to the processing of their Personal Data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract

- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child)

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from the Data Protection Team before any such processing commences.

In any circumstance where consent has not been gained for the specific processing in question, AlertSystems Group Limited shall address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the Personal Data was collected:

- Any link between the purpose for which the Personal Data was collected and the reasons for intended further processing.
- The context in which the Personal Data has been collected, in particular regarding the relationship between Data Subject and the Data Controller.
- The natures of the Personal Data, in particular whether special categories of data are being processed, or whether Personal Data related to criminal convictions and offences are being processed.
- The possible consequences of the intended further processing for the Data Subject.
- The existence of appropriate safeguards pertaining to further processing, which may include encryption, pseudonymisation or anonymisation.

4.4.2 Special Categories of Data

AlertSystems Group Limited shall only process special categories of data (also known as sensitive data) where the Data Subject expressly consents to such processing, or where one of the following conditions applies:

- The processing is necessary for the establishment, exercise or defence of legal claims.
- The processing is specifically authorised or required by law.
- The processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.
- Further conditions, including limitations, based upon national law related to the processing of genetic data, biometric data or data concerning health.

In any situation where special categories of data are to be processed, prior approval shall be obtained from the Data Protection Team and the basis for processing clearly documented. Any additional protection measures required shall be adopted.

4.4.3 Data Quality

AlertSystems Group Limited shall adopt all necessary measures to ensure that the Personal Data it collects and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject.

The measures adopted by AlertSystems Group Limited to ensure data quality include:

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification
- Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period

- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required
- Restriction, rather than deletion of Personal Data, insofar as:
    - a law prohibits erasure
    - erasure would impair legitimate interests of the Data Subject
    - the Data Subject disputes that their Personal Data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

4.4.4 Digital Marketing

As a general rule AlertSystems Group Limited will not send promotional or direct marketing material to its customers through digital channels such as mobile phones, email and the Internet, without first obtaining consent. The Data Protection Team must approve any proposed digital marketing campaigns if prior consent from the Data Subject has not been given.

Where Personal Data Processing is approved for digital marketing purposes, the Data Subject shall be informed of their right to object, at any stage, to having their data processed for such purposes. Upon any such Data Subject objection digital marketing related processing of their Personal Data shall immediately cease and their details retained on an opt-out list with a record of their decision, rather than being completely deleted.

It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of consent to carry out digital marketing to individuals provided they are given the opportunity to opt-out.

4.5 Data Retention and Disposal

4.5.1 AlertSystems Group Limited shall not retain Personal Data for a longer period than is necessary in relation to the purposes for which it was originally collected, or further processed.

4.5.2 AlertSystems Group Limited may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the Data Subject.

4.5.3 The retention period for each category of personal data is set out in the Retention of Records Procedure along with the criteria used to determine this period including any statutory obligations AlertSystems Group Limited has to retain the data.

4.5.4 AlertSystems Group Limited's data retention and data disposal procedures (Storage Removal Procedure) shall apply in all cases.

4.5.5 Personal data shall be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of Data Subjects. Any disposal of data will be done in accordance with the Secure Disposal Procedure.

4.6 Data Protection

4.6.1 AlertSystems Group Limited shall process Personal Data in a manor adopting physical, technical, and organisational measures to ensure the security of Personal Data.

The Data Protection Team shall consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on AlertSystems Group Limited itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical measures, the Data Protection Team shall consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops);
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to AlertSystems Group Limited.

When assessing appropriate organisational measures the Data Protection Team shall consider the following:

- The appropriate training levels throughout AlertSystems Group Limited;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable in a secure environment;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data.

4.6.2 All Employees/Staff are responsible for ensuring any Personal Data that AlertSystems Group Limited holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by AlertSystems Group Limited to receive that information and has entered into a confidentiality agreement.

4.6.3 All Personal Data shall be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. All Personal Data shall be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements in the Access Control Policy and/or
- stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media and Manual Records.

4.6.4 Care shall be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of AlertSystems Group Limited. All Employees/Staff are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs.

4.6.5 Manual records shall not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with the Secure Disposal of Storage procedure.

4.6.6 Personal Data may only be deleted or disposed of in line with the Retention of Records Procedure. Manual records that have reached their retention date are to be shredded and disposed of as

'confidential waste '. Hard drives of redundant PCs are to be removed and immediately destroyed as required by the Secure Disposal of Storage procedure before disposal.

4.6.7 Processing of Personal Data 'off-site' presents a potentially greater risk of loss, theft or damage to Personal Data. Staff must be specifically authorised to process data off-site.

4.7 Data Subject's rights

4.7.1 Data Subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed
- To prevent processing likely to cause damage or distress
- To prevent processing for purposes of direct marketing
- To be informed about the mechanics of automated decision-taking process that will significantly affect them
- To not have significant decisions that will affect them taken solely by automated process
- To sue for compensation if they suffer damage by any contravention of the GDPR
- To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data
- To request the supervisory authority to assess whether any provision of the GDPR has been contravened
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

4.7.2 AlertSystems Group Limited ensures that data subjects may exercise these rights:

- Data subjects may make data access requests as described in Subject Access Request Procedure; this procedure also describes how AlertSystems Group Limited will ensure that its response to the data access request complies with the requirements of the GDPR.
- Data subjects have the right to complain to AlertSystems Group Limited in relation to the processing of their Personal Data. In such circumstances AlertSystems Group Limited's complaints procedure for the handling of requests and appeals from data subjects shall apply.

All requests received for access to or rectification of Personal Data must be directed to the Compliance Manager, who will log each request as it is received. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require AlertSystems Group Limited to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If the Compliance Manager cannot respond fully to the request within 30 days, they shall nevertheless provide the following information to the Data Subject or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request
- Any information located to date
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision
- An estimated date by which any remaining responses will be provided
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature)
- The name and contact information of the Compliance Manager who the Data Subject should contact for follow up.

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information shall be redacted or withheld as may be necessary or appropriate to protect that person's rights.

Detailed guidance for dealing with requests from Data Subjects can be found in the AlertSystems Group Limited Subject Access Request Procedure.

4.8 Disclosure of Data

AlertSystems Group Limited shall ensure that Personal Data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees/Staff shall exercise caution when asked to disclose Personal Data held on another individual to a third party and will be required to attend training that enables them to deal effectively with any such risk. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of AlertSystems Group Limited's business.

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime
- The apprehension or prosecution of offenders
- The assessment or collection of a tax or fine
- By the order of a court or by any rule of law.

All requests to provide data for any of the above reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Compliance Manager.

4.9 Data Transfers

4.9.1 AlertSystems Group Limited may transfer Personal Data to third party recipients but only where one of the following scenarios applies:

- The Data Subject has given consent to the proposed transfer
- The transfer is necessary for the performance of a contract with the Data Subject
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject
- The transfer is legally required on important public interest grounds
- The transfer is necessary for the establishment, exercise or defence of legal claims
- The transfer is necessary in order to protect the vital interests of the Data Subject

4.9.2 AlertSystems Group Limited shall only transfer Personal Data to, or allow access by, third parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where third party processing takes place AlertSystems Group Limited shall first identify if, under applicable law, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

4.9.3 Where the third party is deemed to be a Data Controller AlertSystems Group Limited shall enter into an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred.

4.9.4 Where the third party is deemed to be a Data Processor, AlertSystems Group Limited shall enter into an adequate processing agreement with the Data Processor. The agreement shall require the Data Processor to protect the Personal Data from further disclosure and to only process Personal Data in compliance with AlertSystems Group Limited instructions. In addition, the agreement shall require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches.

4.9.5 When AlertSystems Group Limited outsources services to a third party (including Cloud Computing services), they shall identify whether the third party will process Personal Data on its behalf and whether the outsourcing will entail any third country transfers of Personal Data. In either case, it shall make sure to include adequate provisions in the outsourcing agreement for such processing and third country transfers.

4.9.6 The Data Protection team shall conduct regular audits of processing of Personal Data performed by third parties, especially in respect of technical and organisational measures they have in place. Any major deficiencies identified shall be reported to and monitored by the AlertSystems Group Limited Compliance Manager.

4.10 Complaints Handling

Data Subjects with a complaint about the processing of their Personal Data should put forward the matter in writing to the Compliance Manager compliance.manager@alertsystems.co.uk.
An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Compliance Manager shall inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data Subject and the Compliance Manager, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Information Commissioner's Office.

4.11 Breach Reporting

Any individual who suspects that a Personal Data breach has occurred due to the theft or exposure of Personal Data must immediately notify the Data Protection Team providing a description of what occurred. Notification of the incident can be made via e-mail; compliance.manager@alertsystems.co.uk , or by calling 01225775666.

The Data Protection Team shall investigate all reported incidents to confirm whether or not a Personal Data breach has occurred. If a Personal Data breach is confirmed, the Data Protection Team shall follow the relevant authorised procedure. For severe Personal Data breaches, the Compliance Manager shall initiate and chair an emergency response team to coordinate and manage the Personal Data breach response.

5. Information asset register/data inventory

5.1.1 AlertSystems Group Limited has undertaken data analysis as part of its approach to address risks and opportunities throughout its GDPR compliance project. This analysis has identified:

- business processes that use personal data;
- sources of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of the AlertSystems Group Limited throughout the data flow;
- key systems and repositories;
- any data transfers ; and
- all retention and disposal requirements.

5.1.2 AlertSystems Group Limited is aware of any risks associated with the processing of particular types of personal data.

- AlertSystems Group Limited assesses the level of risk to individuals associated with the processing of their Personal Data. Where applicable data protection impact assessments (DPIAs) shall be carried out

in relation to the processing of Personal Data by AlertSystems Group Limited, and in relation to processing undertaken by other organisations on behalf of AlertSystems Group Limited.

- AlertSystems Group Limited shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.
- Where a type of processing, in particular using new technologies and taking into 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, AlertSystems Group Limited shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of Personal Data. A single DPIA may address a set of similar processing operations that present similar high risks.
- Where, as a result of a DPIA it is clear that AlertSystems Group Limited is about to commence processing of personal data that could cause damage and/or distress to the Data Subjects, the decision as to whether or not AlertSystems Group Limited may proceed must be escalated for review to the Compliance Manager.
- The Compliance Manager shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the Information Commissioner's Office.
- Appropriate controls will be applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to AlertSystems Group Limited's documented risk acceptance criteria and the requirements of the GDPR.

6. Policy Maintenance

All inquiries about this policy, including requests for exceptions or changes should be directed to the Compliance Manager via e-mail compliance.manager@alertsystems.co.uk

7. Related Documents

Listed below are documents that relate to and are referenced by this policy.

- Training policy
- Privacy procedure
- Subject Access Request procedure
- Retention of records procedure
- Data Breach notification
- Data portability
- Consent procedure
- Complaints procedure
- Competence
- Continual improvement procedure
- Access Control policy
- Secure disposal of Storage media policy

Document Owner and Approval

The Compliance Manager is the owner of this document and responsible for ensuring that this policy document is reviewed via the internal audit and Management Review program. This policy is approved by the Board of Directors.

A current version of this document is available to all members of staff on request.

Change History Record

Issue	Description of Change	Approval	Date of Issue

Our Business is Protecting Yours