Integrated Connections

General Data Protection Regulation (GDPR) Compliance Manual

Revision Original

February 10, 2021

Table of Contents

Record of Revisions 5

Highlight of Changes 6

1 Data Protection 7

1.1 Policy Statement 7

1.2 Purpose 7

1.3 Scope 8

1.3.1 Definitions 8

1.4 Data Protection Laws 9

1.4.1 General Data Protection Regulation (GDPR) 9

1.4.2 Data Protection Officer 11

1.5 Objectives 12

1.6 Governance Procedures 13

1.6.1 Accountability & Compliance 13

1.6.2 Legal Basis for Processing (Lawfulness) 15

1.6.3 Third-Party Processors 17

1.6.4 Data Retention & Disposal 17

1.7 Data Protection Impact Assessments (DPIA) 17

1.8 Data Subject Rights Procedures 18

1.8.1 Consent & The Right to be Informed 18

1.8.2 Privacy Notice 19

1.8.3 Personal Data Not Obtained from the Data Subject 19

1.8.4 The Right of Access 19

1.8.5 Data Portability 21

1.8.6 Rectification & Erasure 21

1.8.7 The Right to Restrict Processing 22

1.8.8 Objections and Automated Decision Making 23

1.9 Oversight Procedures 24
1.9.1 Security & Breach Management 24
1.10 Transfers & Data Sharing 24
1.11 Self-Assessments & Monitoring 24
1.12 Training 25
1.13 Penalties 25
1.14 Responsibilities 26
2 Data Retention and Erasure Policy 26
2.1 Policy Statement 26
2.2 Purpose 27
2.3 Scope 27
2.4 Personal Information and Data Protection 27
2.5 Objectives 28
2.6 Guidelines & Procedures 29
2.6.1 Retention Period Protocols 30
2.6.4 Suspension of Record Disposal for Litigation or Claims 30
2.6.5 Storage & Access of Records and Data 30
2.7 Expiration of Retention Period 30
2.7.1 Destruction and Disposal Of Records & Data 30
2.8 Erasure 32
2.9 Compliance and Monitoring 34
2.10 Responsibilities 34
2.11 Retention Periods 34
2.12 Retention Register 35
3 International Data Transfer Policy 37
3.1 Policy Statement 37
3.2 Purpose 37
3.3 Scope 37

3.4 Objectives 37
3.5 Guidelines & Procedures 38
3.5.1 Adequacy Decision 38
3.5.2 Appropriate Safeguards 38
3.5.3 Transfer Exceptions 38
3.6 Responsibilities 39
4 Subject Access Request Procedures 39
4.1 Introduction 39
4.1.1 The General Data Protection Regulation 39
4.2 What is Personal Information? 40
4.3 The Right of Access 40
4.3.1 How To Make a SAR? 41
4.3.2 What We Do When We Receive An Access Request 41
4.4 Fees and Timeframes 42
4.5 Your Other Rights 42
4.6 Exemptions and Refusals 42
4.7 Submission & Lodging a Complaint 43
4.7.1 Supervisory Authority 43
5 Data Breach Policy and Procedures 46
5.1 Policy Statement 46
5.2 Purpose 46
5.3 Scope 46
5.4 Data Security & Breach Requirements 46
5.4.1 Objectives 46
5.5 Data Breach Procedures & Guidelines 47
5.5.1 Breach Monitoring & Reporting 47
1.5.2 Breach Incident Procedures 48
5.5.3 Breach Risk Assessment 49

5.6 Breach Notifications 50
5.6.1 Supervisory Authority Notification 50
5.6.2 Data Subject Notification 51
5.7 Record Keeping 52
5.8 Responsibilities 52
6 Data Breach Incident Form 52

Record of Revisions

Number	Pages	Date	Date Entered	Entered By
Original	ALL	DRAFT	DRAFT	SJB

Highlight of Changes

Revision Number	Description of Changes

1 Data Protection

1.1 Policy Statement

Integrated Connections, LLC *(hereinafter referred to as the **"Company")*** needs to collect personal information to effectively carry out our everyday business functions and activities and to provide the products and services defined by our business type. Such data is collected from employees, customers, suppliers and clients and includes *(but is not limited to)*, name, address, email address, data of birth, IP address, identification numbers, private and confidential information, sensitive information.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to processing all personal information in accordance with the ***General Data Protection Regulation (GDPR)*** and any other relevant the data protection laws and codes of conduct (*herein collectively referred to as "**the data protection laws**"*).

The Company has developed policies, procedures, controls and measures to ensure continued compliance with the data protection laws and principles, including staff training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and confidentiality of personal and/or special category data is one of our top priorities and we are proud to operate a ***'Privacy by Design'*** approach, assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.

1.2 Purpose

The purpose of this policy is to ensure that the Company meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed compliantly.

The data protection laws include provisions that promote accountability and governance and as such the Company has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimize the risk of breaches and uphold the protection of personal data. This policy also serves as a reference document for employees and third-parties on the responsibilities of handling and accessing personal data and data subject requests.

1.3 Scope

This policy applies to all staff within the Company *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the US or overseas)*, but only with respect to data that is affected by the GDPR (i.e. data collected from EU residents, or other persons who have significant contact with the EU). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

1.3.1 Definitions

"Biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

"Binding Corporate Rules" means personal data protection policies which are adhered to by the Company for transfers of personal data to a controller or processor in one or more third countries or to an international organization.

"Consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

"Cross Border Processing" means processing of personal data which: takes place in more than one Member State; or which substantially affects or is likely to affect data subjects in more than one Member State

"Data controller" means, the 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

"Data processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

"Data protection laws" means for the purposes of this document, the collective description of the GDPR, Data Protection Act 2018 (*referred to as the Act*) and any other relevant data protection laws that the Company complies with.

"Data subject" means an individual who is the subject of personal data; and is either a resident of the EU or who has data that is collected/processed or otherwise touched by entities within the EU.

"GDPR" means the *General Data Protection Regulation (EU) (2016/679).*

"Genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

"Personal data" means 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.

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

"Recipient" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third-party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

"Supervisory Authority" means an independent public authority which is established by a Member State.

"Third Party" means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority.

1.4 Data Protection Laws

1.4.1 General Data Protection Regulation (GDPR)

The ***General Data Protection Regulation (GDPR) (EU)2016/679)*** was approved by the European Commission in April 2016 and will apply to all EU Member States after May 25, 2018. As a *'Regulation*' rather than a *'Directive'*, its rules apply directly to Member States, replacing their existing local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation.

As the Company processes personal information regarding individuals who are residents or have significant contacts with the EU (*data subjects*), we are obligated under the General

Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, in compliance with its rules and principles.

1.4.1.1 Personal Data

Information protected under the GDPR is known as *"personal data"* and is defined as: -

"Any information relating to an identified or identifiable natural person; 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."

The Company ensures that a high level of care is afforded to personal data falling within the GDPR's **'special categories'** *(previously **sensitive personal data***), due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

In relation to the 'Special categories of Personal Data' the GDPR advises that: -

"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies."

1.4.1.2 The GDPR Principles

Article 5 of the GDPR requires that personal data shall be: -

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ***('lawfulness, fairness and transparency')***

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ***('purpose limitation')***

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ***('data minimization')***

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ***('accuracy')***

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ***('storage limitation')***

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ***('integrity and confidentiality').***

Article 5(2) requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles'* ***('accountability')*** and requires that firms ***show how*** they comply with the principles, detailing and summarizing the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

1.4.2 Data Protection Officer

Articles 37-39, and Recital 97 of the GDPR detail the obligations, requirements and responsibilities on firms to appoint a Data Protection Officer and specifies the duties that the officer themselves must perform.

A Data Protection Officer (DPO) must be appointed by a firm where: -

- The processing is carried out by a public authority or body *(except for courts acting in their judicial capacity)*
- the core activities of the controller/processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale
- the core activities of the controller/processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offenses referred to in Article 10

Where the Company has appointed a designated **DPO,** we have done so in accordance with the GDPR requirements and have ensured that the assigned person has an adequate and expert knowledge of data protection law. They have been assessed as being fully capable of assisting the Company in monitoring our internal compliance with the Regulation and supporting and advising employees and associated third parties with regards to the data protection laws and requirements.

For the DPO duties and responsibilities, please refer to our DPO Responsibilities

document.

1.5 Objectives

We are committed to ensuring that all personal data processed by the Company is done so in accordance with the data protection laws and its principles, along with any associated regulations and/or codes of conduct laid down by the Supervisory Authority and local law. We ensure the safe, secure, ethical and transparent processing of all personal data and have stringent measures to enable data subjects to exercise their rights.

The Company has developed the below objectives to meet our data protection obligations and to ensure continued compliance with the legal and regulatory requirements.

The Company ensures that: -

- We protect the rights of individuals with regards to the processing of personal information
- We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with the data protection laws
- Every business practice, function and process carried out by the Company, is monitored for compliance with the data protection laws and its principles
- Personal data is only processed where we have verified and met the lawfulness of processing requirements
- We only process special category data in accordance with the GDPR requirements and in compliance with the Data Protection Act 2018 Schedule 1 conditions
- We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested
- All employees are competent and knowledgeable about their GDPR obligations and are provided with training in the data protection laws, principles, regulations and how they apply to their specific role and the Company
- Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection laws
- We maintain a continuous program of monitoring, review and improvement with regards to compliance with the data protection laws and to identify gaps and non-compliance before they become a risk, affecting mitigating actions where necessary
- We monitor the Supervisory Authority, European Data Protection Board (EDPB) and any GDPR news and updates, to stay abreast of changes, notifications and additional requirements
- We have a documented Complaint Handling and Data Breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection

- We have appointed a **Data Protection Officer** who takes responsibility for the overall supervision, implementation and ongoing compliance with the data protection laws and performs specific duties as set out under Article 37 of the GDPR
- We have a dedicated Audit & Monitoring Program in place to perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared. The audit program is reviewed against our data protection policies, procedures and the relevant regulations to ensure continued compliance
- We provide clear reporting lines and supervision with regards to data protection
- We store and destroy all personal information, in accordance with our retention policy and schedule which has been developed from the legal, regulatory and statutory requirements and suggested timeframes
- Any information provided to an individual in relation to personal data held or used about them, with be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language
- Employees are aware of their own rights under the data protection laws and are provided with the Article 13/14 information disclosures in the form of a Privacy Notice
- Where applicable, we maintain records of processing activities in accordance with the Article 30 requirements
- We have developed and documented appropriate technical and organizational measures and controls for personal data security and have a robust Information Security program in place

1.6 Governance Procedures

1.6.1 Accountability & Compliance

Due to the nature, scope, context and purposes of processing undertaken by the Company, we carry out risk assessments and information audits to identify, assess, measure and monitor the impact of such processing. We have implemented adequate and appropriate technical and organizational measures to ensure the safeguarding of personal data and compliance with the data protection laws and can evidence such measures through our documentation and practices.

Our main governance objectives are to: -

- Educate Senior Management and employees about the requirements under the data protection laws and the possible impact of non-compliance
- Provide a dedicated and effective data protection training program for all employees
- Identify key stakeholders to support the data protection compliance program
- Allocate responsibility for data protection compliance and ensure that the

designated person(s) has sufficient access, support and budget to perform the role

- Identify, create and disseminate the reporting lines within the data protection governance structure

The technical and organizational measures that the Company has in place to demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated information security policies.

1.6.1.1 Privacy by Design

We operate a *'Privacy by Design'* approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. We have developed controls and measures *(detailed below*), that help us enforce this ethos.

Data Minimization

Under Article 5 of the GDPR, principle (c) advises that data should be *'limited to what is necessary'*, which forms the basis of our minimalist approach. We only ever obtain, retain, process and share the data that is essential for carrying out our services and/or meeting our legal obligations and only retain data for as long as is necessary.

Our systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimization enables us to reduce data protection risks and breaches and supports our compliance with the data protection laws.

Encryption

We utilize encryption as a further risk prevention measure for securing the personal data that we hold. Encryption with a secret key is used to make data indecipherable unless decryption of the dataset is carried out using the assigned key.

We utilize encryption via secret key for transferring personal data to any external party and provide the secret key in a separate format. Where special category information is being transferred and/or disclosed, the Data Protection Officer is required to authorize the transfer and review the encryption method for compliance and accuracy.

Restriction

Our *Privacy by Design* approach means that we use Company-wide restriction methods for all personal data activities. Restricting access is built into the foundation of the Company's processes, systems and structure and ensures that only those with authorization and/or a relevant purpose, have access to personal information.

Hard Copy Data

Due to the nature of our business, it is sometimes essential for us to obtain, process and share personal and special category information which is only available in a paper format without pseudonymization options (*i.e. copies of patient records, hospital invoices or claims information*).

1.6.2 Legal Basis for Processing (Lawfulness)

At the core of all personal information processing activities undertaken by the Company, is the verification that we are complying with Article 6 of the GDPR and our lawfulness of processing obligations. Prior to carrying out any personal data processing activity, we identify and establish the legal basis for doing so and verify these against the regulation requirements to ensure we are using the most appropriate legal basis.

The legal basis is documented on our information audit register and in our Privacy Notice and, where applicable, is provided to the data subject and Supervisory Authority as part of our information disclosure obligations. ***Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where: -***

- 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 we are 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 or in the exercise of official authority vested in the Company
- Processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third-party

1.6.2.1 Processing Special Category Data

Special categories of Personal Data are defined in the data protection laws as: -

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies.

Where the Company processes any personal information classed as special category or information relating to criminal convictions, we do so in accordance with Article 9 of the

GDPR regulations and in compliance with the Data Protection Act 2018 Schedule 1 Parts 1, 2, 3 & 4 conditions and requirements.

We will only ever process special category data where: -

- The data subject (or his or her designee) has given explicit consent to the processing of the personal
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- 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
- Processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

Schedule 1, Parts 1, 2 & 3 of The Data Protection Act 2018 provide specific conditions and circumstances when special category personal data can be processed and details the requirements that organizations are obligated to meet when processing such data.

Where the Company processes personal information that falls into one of the above categories, we have adequate and appropriate provisions and measures in place prior to any processing. ***Measures include: -***

- Verifying our reliance on one of the data protection laws Article 9(1), and where applicable The Data Protection Act 2018 Sch.1, Pt.1, Pt.2 and/or Pt.3 conditions prior to processing
- Documenting the Schedule 1 condition and Article 6(1) legal basis relied upon from processing on our Processing Activities Register (*where applicable)*
- Having an appropriate policy document in place when the processing is carried out, specifying our: -
  - procedures for securing compliance with the data protection laws principles
  - policies as regards the retention and erasure of personal data processed in reliance on the condition
  - retention periods and reason *(i.e. legal, statutory etc)*
  - procedures for reviewing and updating our policies in this area

Please refer to our Retention & Erasure Policy for further guidance and procedures.

1.6.3 Third-Party Processors

The Company utilize external processors for certain processing activities *(where applicable*). We use information audits to identify, categorize and record all personal data that is processed outside of the Company, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible.

We have due diligence and Know Your Customer procedures and measures in place and review, assess and background check all processors prior to forming a business relationship. We obtain company documents, certifications, references and ensure that the processor is adequate, appropriate and effective for the task we are employing them for.

The continued protection of data subjects' rights and the security of their personal information is always our top priority when choosing a processor and we understand the importance of adequate and reliable outsourcing for processing activities as well as our continued obligations under the data protection laws for data processed and handled by a third-party.

1.6.4 Data Retention & Disposal

The Company have defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and our business requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects *(e.g. shredding, disposal as confidential waste, secure electronic deletion)* and prioritizes the protection of the personal data in all instances.

Please refer to our ***Data Retention & Erasure Policy*** for full details on our retention, storage, periods and destruction processes.

1.7 Data Protection Impact Assessments (DPIA)

Individuals have an expectation that their privacy and confidentiality will be upheld and respected while their data is being stored and processed by the Company. We therefore utilize several measures and tools to reduce risks and breaches for general processing. However, where processing is likely to be high risk or cause significant impact to a data subject, we utilize proportionate methods to map out and assess the impact ahead of time.

Where the Company must or are considering carrying out processing that utilizes new technologies, and/or where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, we always carry out a Data Protection Impact Assessment (DPIA) *(sometimes referred to as a Privacy Impact Assessment*).

1.8 Data Subject Rights Procedures

1.8.1 Consent & The Right to be Informed

The collection of personal and sometimes special category data is a fundamental part of the products/services offered by the Company and we therefore have specific measures and controls in place to ensure that we comply with the conditions for consent under the data protection laws.

The data protection law defines consent as; *'Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.*

Where processing is based on consent, the Company have reviewed and revised all consent mechanisms to comply with such consent. Consent Controls

The Company maintain records of data subject consent for processing personal data and are always able to demonstrate that the data subject has consented to processing of his or her personal data where applicable. We also ensure that the withdrawal of consent is as clear, simple and transparent and is documented in all instances.

Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from those matters, in an intelligible and easily accessible form, using clear and plain language. All such written declarations are reviewed and authorized by the Data Protection Officer prior to being circulated.

Consent to obtain and process personal data is obtained by the Company through: -

- Face-to-Face
- Telephone
- In Writing
- Email/SMS
- Electronic *(i.e. via website form*)

Any electronic methods of gaining consent are regularly reviewed and tested to ensure that a compliant Privacy Notice is accessible and displayed and that consent is clear, granular and utilizes a demonstrable opt-in mechanism. Where consent is obtained verbally, we utilize scripts, checklists to ensure that all requirements have been met and that consent is obtained compliantly and can be evidenced.

Privacy Notices are used in all forms of consent and personal data collection, to ensure that we are compliant in disclosing the information required in the data protection laws in an easy to read and accessible format.

1.8.1.2 Information Provisions

Where personal data is obtained directly from the individual *(i.e. through consent, by employees, written materials and/or electronic formats (i.e. website forms, subscriptions, email etc*)), we provide the below information in all instances, **in the form of our Notice of Privacy Practices on our website.**

1.8.2 Privacy Notice

The Company defines a Privacy Notice as a document, form, webpage or pop-up that is provided to individuals at the time we collect their personal *data (or at the earliest possibility where that data is obtained indirectly)*.

Our Privacy Notice includes the Article 13 (*where collected directly from individual*) or *14 (where not collected directly)* requirements and provides individuals with all the necessary and legal information about how, why and when we process their data, along with their rights and obligations.

We have a link to our Privacy Notice on our website and provide a copy of physical and digital formats upon request. The notice is the customer facing policy that provides the legal information on how we handle, process and disclose personal information.

The notice is easily accessible, legible, jargon-free and is via our website (and as part of the pre-flight package provided to our clients)

1.8.3 Personal Data Not Obtained from the Data Subject

Where the Company obtains and/or processes personal data that has **not** been obtained directly from the data subject, the Company ensures that the information disclosures contain in Article 14 are provided to the data subject.

1.8.4 The Right of Access

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13/14 and any communication under Articles 15 to 22 and 34 *(collectively, The Rights of Data Subjects*), in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided free of charge and is in writing, or by other means where authorized by the data subject and with prior verification as to the subject's identity *(i.e. verbally, electronic*).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

1.8.4.1 Subject Access Request

Where a data subject asks us to confirm whether we hold and process personal data concerning him or her and requests access to such data; we provide them with: -

- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be disclosed
- If the data has or will be disclosed to a third countries or international organizations and the appropriate safeguards pursuant to the transfer
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint with a Supervisory Authority
- Where personal data has not been collected by the Company from the data subject, any available information as to the source and provider
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Subject Access Requests (SAR) are passed to the **Data Protection Officer** as soon as received and a record of the request is noted. The type of personal data held about the individual is checked against our Information Audit to see what format it is held in, who else has it has been shared with and any specific timeframes for access.

SARs are always completed within 30-days and are provided free of charge. Where the individual makes the request by electronic means, we provide the information in a

commonly used electronic format, unless an alternative format is requested.

Please refer to our external ***Subject Access Request Procedures*** for the guidelines on how an SAR can be made and what steps we take to ensure that access is provided under the data protection laws.

1.8.5 Data Portability

The Company provides all personal information pertaining to the data subject to them on request and in a format, that is easy to disclose and read. We ensure that we comply with the data portability rights of individuals by ensuring that all personal data is readily available and is in a structured, commonly used and machine-readable format, enabling data subjects to obtain and reuse their personal data for their own purposes across different services.

All requests for information to be provided to the data subject or a designated controller are done so free of charge and within 30 days of the request being received. If for any reason, we do not act in responding to a request, we provide a full, written explanation within 30 days to the data subject or the reasons for refusal and of their right to complain to the Supervisory Authority and to a judicial remedy.

1.8.6 Rectification & Erasure

1.8.6.1Correcting Inaccurate or Incomplete Data

Pursuant to Article 5(d), all data held and processed by the Company is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject or controller inform us that the data we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

The **Data Protection Officer** is notified of the data subjects request to update personal data and are responsible for validating the information and rectifying errors where they have been notified. The information is altered as directed by the data subject, with the information audit being checked to ensure that all data relating to the subject is updated where incomplete or inaccurate. Once updated, we add an addendum or supplementary statement where applicable.

Where notified of inaccurate data by the data subject, we will rectify the error within 30 days and inform any third-party of the rectification if we have disclosed the personal data in question to them. The data subject is informed in writing of the correction and where applicable, is provided with the details of any third-party to whom the data has been disclosed.

If for any reason, we are unable to act in response to a request for rectification and/or completion, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

1.8.6.2 The Right to Erasure

Also, known as *'The Right to be Forgotten'*, the Company complies fully with Article 5(e) and ensures that personal data which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed.

All personal data obtained and processed by the Company is categorized when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

Please refer to our Data Retention & Erasure Policy for exact procedures on erasing data and complying with the Article 17 requirements.

1.8.7 The Right to Restrict Processing

There are certain circumstances where the Company restricts the processing of personal information, to validate, verify or comply with a legal requirement of a data subjects request. Restricted data is removed from the normal flow of information and is recorded as being restricted on the information audit.

Any account and/or system related to the data subject of restricted data is updated to notify users of the restriction category and reason. When data is restricted it is only stored and not processed in any way.

The Company will apply restrictions to data processing in the following circumstances: -

- Where an individual contest the accuracy of the personal data and we are in the process verifying the accuracy of the personal data and/or making corrections
- Where an individual has objected to the processing (*where it was necessary for the performance of a public interest task or purpose of legitimate interests*), and we are considering whether we have legitimate grounds to override those of the individual
- When processing is deemed to have been unlawful, but the data subject requests restriction as opposed to erasure
- Where we no longer need the personal data, but the data subject requires the data to establish, exercise or defend a legal claim

The Data Protection Officer reviews and authorizes all restriction requests and actions and retains copies of notifications from and to data subjects and relevant third-parties. Where data is restricted, and we have disclosed such data to a third-party, we will inform the third-party of the restriction in place and the reason and re-inform them if any such restriction is lifted.

Data subjects who have requested restriction of data are informed within 30 days of the restriction application and are also advised of any third-party to whom the data has been disclosed. We also provide in writing to the data subject, any decision to lift a restriction on processing. If for any reason, we are unable to act in response to a request for restriction, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

1.8.8 Objections and Automated Decision Making

Data subjects are informed of their right to object to processing in our Privacy Notices and at the point of first communication, in a clear and legible form and separate from other information. We provide opt-out options on all direct marketing material and provide an online objection form where processing is carried out online. ***Individuals have the right to object to: -***

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority *(including profiling*)
- Direct marketing (*including profiling*)
- Processing for purposes of scientific/historical research and statistics

Where the Company processes personal data for the performance of a legal task, in relation to our legitimate interests or for research purposes, a data subjects' objection will only be considered where it is on *'grounds relating to their particular situation'*. We reserve the right to continue processing such personal data where: -

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- The processing is for the establishment, exercise or defense of legal claims

Where we are processing personal information for direct marketing purposes under a previously obtained consent, we will stop processing such personal data immediately where an objection is received from the data subject. This measure is absolute, free of charge and is always adhered to.

Where a data subject objects to data processing on valid grounds, the Company will cease the processing for that purpose and advise the data subject of cessation in writing within 30 days of the objection being received.

1.9 Oversight Procedures

1.9.1 Security & Breach Management

Alongside our *'Privacy be Design'* approach to protecting data, we ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred. Our ***Information Security Policies*** provide the detailed measures and controls that we take to protect personal information and to ensure its security from consent to disposal.

We carry out self-assessments to ensures that all personal data held and processed by us is accounted for and recorded, alongside risk assessments as to the scope and impact a data breach could have on data subject(s). We have implemented adequate and appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

While every effort and measure are taken to reduce the risk of data breaches, the Company has dedicated controls and procedures in place for such situations, along with the notifications to be made to the Supervisory Authority and data subjects (where applicable).

Please refer to our ***Data Breach Policy & Procedures*** for specific protocols.

1.10 Transfers & Data Sharing

The Company takes proportionate and effective measures to protect personal data held and processed by us at all times, however we recognize the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred.

Where data is being transferred for a legal and necessary purpose, compliant with all Articles in the Regulation, we utilize a process that ensures such data is encrypted with a secret key and where possible is also subject to our data minimization methods.

Please refer to our International Data Transfer Procedures for further details.

1.11 Self-Assessments & Monitoring

This policy and procedure document details the controls, measures and methods used by the Company to protect personal data, uphold the rights of data subjects, mitigate risks, minimize breaches and comply with the data protection laws and associated laws and codes of conduct. In addition to these, we also carry out regular audits and compliance monitoring processes

with a view to ensuring that the measures and controls in place to protect data subjects and their information, are adequate, effective and compliant at all times.

The Data Protection Officer has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place and reporting improvement action plans to the Senior Management Team where applicable. Data minimization methods are reviewed and new technologies assessed to ensure that we are protecting data and individuals.

The aim of self-assessments is to: -

- Ensure that the appropriate policies and procedures are in place
- To verify that those policies and procedures are being followed
- To test the adequacy and effectiveness of the measures and controls in place
- To detect breaches or potential breaches of compliance
- To identify risks and assess the mitigating actions in place to minimize such risks
- To recommend solutions and actions plans to Senior Management for improvements in protecting data subjects and safeguarding their personal data
- To monitor compliance with the data protection laws and demonstrate best practice

1.12 Training

Through our strong commitment and robust controls, we ensure that all staff understand, have access to and can easily interpret the data protection laws requirements and its principles and that they have ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role. Our ***Training & Development Policy & Procedures*** and ***Induction Policy*** detail how new and existing employees are trained, assessed and supported and include.

1.13 Penalties

The Company understands its obligations and responsibilities under the data protection laws and recognizes the severity of breaching any part of the law or Regulation. We respect the Supervisory Authority's authorization under the legislation to impose and enforce fines and penalties on us where we fail to comply with the regulations, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees have been made aware of the severity of such penalties and their proportionate nature in accordance with the breach. ***We recognize that: -***

- Breaches of the obligations of the controller, the processor, the certification body and the monitoring body, are subject to administrative fines up to €10,000,000 or 2 % of the total

worldwide annual turnover of the preceding financial year, whichever is higher.

• Breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organization, specific processing situations (*Chapter IX*) or non-compliance with an order by the Supervisory Authority, are subject to administrative fines up to €20,000,000 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

1.14 Responsibilities

The Company has appointed a **Data Protection Officer** whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

The DPO has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the data protection laws and our own internal objectives and obligations.

2. Data Retention and Erasure Policy

2.1 Policy Statement

Integrated Connections, Inc. *(hereinafter referred to as the **"Company"**)* recognizes that the efficient management of its data and records is necessary to support its core business functions, to comply with its legal, statutory and regulatory obligations, to ensure the protection of personal information and to enable the effective management of the organization.

This policy and related documents meet the standards and expectations set out by contractual and legal requirements and has been developed to meet the best practices of business records management, with the aim of ensuring a structured approach to document control.

Effective and adequate records and data management is necessary to: -

• Ensure that the business conducts itself in a structured, efficient and accountable manner

• Ensure that the business realizes best value through improvements in the quality and flow of information and greater coordination of records and storage systems

• Support core business functions and provide evidence of conduct and the appropriate maintenance of systems, tools, resources and processes

• Meet legislative, statutory and regulatory requirements

- Deliver services to, and protect the interests of, employees, clients and stakeholders in a consistent and equitable manner
- Assist in document policy formation and managerial decision making
- Provide continuity in the event of a disaster or security breach
- Protection personal information and data subject rights
- Avoid inaccurate or misleading data and minimize risks to personal information
- Erase data in accordance with the legislative and regulatory requirements

Information held for longer than is necessary carries additional risk and cost and can breach data protection rules and principles. The Company only ever retains records and information for legitimate or legal business reasons and always comply fully with the data protection laws, guidance and best practice.

2.2 Purpose

The purpose of this document is to provide the Company's statement of intent on how it provides a structured and compliant data and records management system. We define ***'records'*** as all documents, regardless of the format; which facilitate business activities, and are thereafter retained to provide evidence of transactions and functions.

Such records may be created, received or maintained in hard copy or in an electronic format with the overall definition of records management being a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and disposal of records.

2.3 Scope

This policy applies to all staff within the Company *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the US or overseas).* Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

2.4 Personal Information and Data Protection

The Company needs to collect personal information about the people we employ, work with have a business relationship with, to effectively and compliantly carry out our everyday business functions and activities, and to provide the products and services defined by our business type. This information can include *(but is not limited to),* name, address, email address, data of birth, IP address, identification number, private and confidential information, sensitive information and bank details.

In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to collecting, processing, storing and destroying all information in accordance with the ***General Data Protection Regulation***, US data protection laws and any other associated legal or regulatory body rules or codes of conduct that apply to our business and/or the information we process and store.

Our Data Retention Policy and processes comply with the GDPR's fifth Article 5 principle:

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ***('storage limitation').***

2.5 Objectives

A record is information, regardless of media, created, received, and maintained which evidences the development of, and compliance with, regulatory requirements, business practices, legal policies, financial transactions, administrative activities, business decisions or agreed actions. It is the Company's objective to implement the necessary records management procedures and systems which assess and manage the following processes: -

- The creation and capture of records
- Compliance with legal, regulatory and contractual requirements
- The storage of records
- The protection of record integrity and authenticity
- The use of records and the information contained therein
- The security of records
- Access to and disposal of records

Records contain information that are a unique and invaluable resource to the Company and are an important operational asset. A systematic approach to the management of our records is essential to protect and preserve the information contained in them, as well as the individuals such information refers to. Records are also pivotal in the documentation and evidence of all business functions and activities.

The Company's objectives and principles in relation to Data Retention are to: -

- Ensure that the Company conducts itself in an orderly, efficient and accountable manner
- Support core business functions and providing evidence of compliant retention, erasure and destruction
- To develop and maintain an effective and adequate records management program to ensure effective archiving, review and destruction of information
- To only retain personal information for as long as is necessary
- Comply with the relevant data protection regulation, legislation and any contractual obligations
- Ensure the safe and secure disposal of confidential data and information assets
- Ensure that records and documents are retained for the legal, contractual and regulatory period stated in accordance with each bodies rules or terms.
- Ensure that no document is retained for longer than is legally or contractually allowed
- Mitigate against risks or breaches in relation to confidential information

2.6 Guidelines & Procedures

The Company manage records efficiently and systematically, in a manner consistent with the GDPR requirements and various state and federal laws. Records management training is mandatory for all staff as part of the Company's statutory and compliance training program and this policy is widely disseminated to ensure a standardized approach to data retention and records management.

Records will be created, maintained and retained to provide information about, and evidence of the Company's transactions, customers, employment and activities. Retention schedules will govern the period that records will be retained and can be found in the ***Record Retention Periods*** table at the end of this document.

It is our intention to ensure that all records and the information contained therein is: -

- **Accurate** - records are always reviewed to ensure that they are a full and accurate representation of the transactions, activities or practices that they document
- **Accessible** - records are always made available and accessible when required (*with additional security permissions for select staff where applicable to the document content*)
- **Complete** - records have the content, context and structure required to allow the reconstruction of the activities, practices and transactions that they document
- **Compliant** - records always comply with any record keeping legal and regulatory requirements

• **Monitored** – staff, Company and system compliance with this Data Retention Policy is regularly monitored to ensure that the objectives and principles are being complied with at all times and that all legal and regulatory requirements are being adhered to.

2.6.1 Retention Period Protocols

All records retained during their specified periods are traceable and retrievable.

2.6.4 Suspension of Record Disposal for Litigation or Claims

If the Company is served with any legal request for records or information, any employee becomes the subject of an audit or investigation or we are notified of the commencement of any litigation against our Company, we will suspend the disposal of any scheduled records until we are able to determine the requirement for any such records as part of a legal requirement.

2.6.5 Storage & Access of Records and Data

Documents are grouped together by category and then in clear date order when stored and/or archived. Documents are always retained in a secure location, with authorized personnel being the only ones to have access. Once the retention period has elapsed, the documents are either reviewed, archived or confidentially destroyed dependent on their purpose, classification and action type.

2.7 Expiration of Retention Period

Once a record or data has reached its designated retention period date, the designated owner should refer to the retention register for the action to be taken. Not all data or records are expected to be deleted upon expiration; sometimes it is sufficient to anonymize the data in accordance with the GDPR requirements or to archive records for a further period.

2.7.1 Destruction and Disposal Of Records & Data

All information of a confidential or sensitive nature on paper, card, microfiche or electronic media must be securely destroyed when it is no longer required. This ensures compliance with the Data Protection laws and the duty of confidentiality we owe to our employees, clients and customers.

The Company is committed to the secure and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner. We confirm that our approach and procedures comply with the laws and provisions made in the General Data Protection Regulation (GDPR) and that staff are trained and advised accordingly on the procedures and controls in place.

2.7.1.1 Paper Records

Due to the nature of our business, the Company retains paper based personal information and as such, has a duty to ensure that it is disposed of in a secure, confidential and compliant manner. The Company utilize shredding service provider to dispose of all paper materials.

Employee shredding machines and confidential waste sacks are made available throughout the building and where we use a service provider for large disposals, regular collections take place to ensure that confidential data is disposed of appropriately.

2.7.1.2 Electronic & IT Records and Systems

The Company uses numerous systems, computers and technology equipment in the running of our business. From time to time, such assets must be disposed of and due to the information held on these while they are active, this disposal is handled in an ethical and secure manner.

The deletion of electronic records must be organized in conjunction with the IT Department who will ensure the removal of all data from the medium so that it cannot be reconstructed. When records or data files are identified for disposal, their details must be provided to the designated owner to maintain an effective and up to date a register of destroyed records.

Only the IT Department can authorize the disposal of any IT equipment and they must accept and authorize such assets from the department personally. Where possible, information is wiped from the equipment through use of software and formatting, however this can still leave imprints or personal information that is accessible and so we also comply with the secure disposal of all assets.

In all disposal instances, the IT Department must complete a disposal form and confirm successful deletion and destruction of each asset. This must also include a valid certificate of disposal from the service provider removing the formatted or shredded asset. Once disposal has occurred, the IT Department is responsible for liaising with the information asset owner and updating the Information Asset Register for the asset that has been removed.

It is the explicit responsibility of the asset owner and IT Department to ensure that all relevant data has been sufficiently removed from the IT device and backed up before requesting disposal and/or prior to the scheduled pickup.

2.7.1.3 Internal Correspondence and General Memorandums

Unless otherwise stated in this policy or the retention periods register, correspondence and internal memorandums should be retained for the same period as the document to

which they pertain or support *(i.e. where a memo pertains to a contract or personal file, the relevant retention period and filing should be observed*).

Where correspondence or memorandums that do not pertain to any documents having already be assigned a retention period, they should be deleted or shredded once the purpose and usefulness of the content ceases or at a maximum, 7 years.

Examples of correspondence and routine memorandums include (but are not limited to):

- Internal emails
- Meeting notes and agendas
- General inquiries and replies
- Letter, notes or emails of inconsequential subject matter

2.8 Erasure

In specific circumstances, data subjects' have the right to request that their personal data is erased, however the Company recognize that this is not an absolute *'right to be forgotten'*. Data subjects only have a right to have personal data erased and to prevent processing if one of the *below conditions applies: -*

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data must be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

Where one of the above conditions applies and the Company received a request to erase data, we first ensure that no other legal obligation or legitimate interest applies. If we are confident that the data subject has the right to have their data erased, this is carried out by the Data Protection Officer in conjunction with any department manager and the IT team to ensure that all data relating to that individual has been erased.

These measures enable us to comply with a data subjects right to erasure, whereby an individual can request the deletion or removal of personal data where there is no

compelling reason for its continued processing. While our standard procedures already remove data that is no longer necessary, we still follow a dedicated process for erasure requests to ensure that all rights are complied with and that no data has been retained for longer than is needed.

Where we receive a request to erase and/or remove personal information from a data subject, the below process is followed: -

1. The request is allocated to the Data Protection Officer and recorded on the Erasure Request Register
2. The DPO locates all personal information relating to the data subject and reviews it to see if it is still being processed and is still necessary for the legal basis and purpose it was originally intended
3. The request is reviewed to ensure it complies with one or more of the grounds for erasure: -
    a. the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
    b. the data subject has withdrawn consent on which the processing is based and where there is no other legal ground for the processing
    c. the data subject objects to the processing and there are no overriding legitimate grounds for the processing
    d. the personal data has been unlawfully processed
    e. the personal data must be erased for compliance with a legal obligation
    f. the personal data has been collected in relation to the offer of information society services to a child
4. If the erasure request complies with one of the above grounds, it is erased within 30 days of the request being received
5. The DPO writes to the data subject and notifies them in writing that the right to erasure has been granted and provides details of the information erased and the date of erasure
6. Where the Company has made any of the personal data public and erasure is granted, we will take every reasonable step and measure to remove public references, links and copies of data and to contact related controllers and/or processors and inform them of the data subjects request to erase such personal data

If for any reason, we are unable to act in response to a request for erasure, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy. ***Such refusals to erase data include: -***

- Exercising the right of freedom of expression and information

- Compliance with a legal obligation for the performance of a task carried out in the public interest
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
- For the establishment, exercise or defense of legal claims

2.9 Compliance and Monitoring

The Company are committed to ensuring the continued compliance with this policy and any associated legislation and undertake regular audits and monitoring of our records, their management, archiving and retention. Information asset owners are tasked with ensuring the continued compliance and review of records and data within their remit.

2.10 Responsibilities

Heads of departments and information asset owners have overall responsibility for the management of records and data generated by their departments' activities, namely to ensure that the records created, received and controlled within the purview of their department, and the systems (*electronic or otherwise*) and procedures they adopt, are managed in a way which meets the aims of this policy.

Where a DPO has been designated, they must be involved in any data retention processes and records or all archiving and destructions must be retained. Individual employees must ensure that the records for which they are responsible are complete and accurate records of their activities, and that they are maintained and disposed of in accordance with the Company's protocols.

2.11 Retention Periods

Section 12 of this policy contains our regulatory, statutory and business retention periods and the subsequent actions upon reaching those dates. Where no defined or legal period exists for a record, the default standard retention period is 6 years plus the current year (*referred to as 6 years + 1*).

2.12 Retention Register

RECORD	RETENTION PERIOD	ASSET OFFICER	ACTION
Information, data or record	*Period for retaining record & accompanying notes*	*Who is responsible for reviewing periods*	*Destroy, archive, review etc*
Accounting records	3 years for private companies	*DPO*	Review
Income tax returns Income tax records	At least 3 years after the end of the financial year to which they relate	*DPO*	Review
Complaints, records, letters, responses & customer communications	3 years for all other complaints	*DPO*	Review
Records documenting the firm's relationships and responsibilities to statutory and/or regulatory bodies and its legal responsibilities	Permanent	*DPO*	Review
Business documents, policies, procedures, strategies etc	Superseded + 6 years *(then reviewed for archive value purposes)*	*DPO*	Review
Supplier, business relationship documents, contracts, SLA's, audits, reviews etc	End of relationship + 6 years	*DPO*	Review
Reviews, analysis, compliance monitoring, quality assurance, operational performance etc	5 years +1	*DPO*	Review
Marketing, promotion, press releases	2 years after last action	*DPO*	Review

Memberships, certification and/or accreditation with professional associations	End of membership/accreditation + 1 year	*DPO*	Review

3. International Data Transfer Policy

3.1 Policy Statement

Integrated Connections, Inc. *(hereinafter referred to as the **"Company"**)* understands that any transfer of personal data undergoing processing or intended for processing after transfer to a third country or an international organization, shall only take place in compliance with Chapter 5 of the GDPR.

This policy is to be read in conjunction with our ***Data Protection Policy*** and provides our procedures for transferring personal data to a third country or international organization. We adhere to the Regulation for all non-EU transfers and have robust transfer safeguarding measures and controls in place to protect the personal data and the rights of the data subject.

3.2 Purpose

The purpose of this policy is to provide our procedures and guidelines for transferring personal data outside the EU for processing and to demonstrate our adherence to the Chapter 5 requirements and compliance with the required safeguarding measures.

3.3 Scope

This policy applies to all staff within the Company *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the US or overseas)*. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

3.4 Objectives

It is the Company's aim to ensure that all personal data transfers to a third country or an international organization comply with the Chapter 5 requirements under the GDPR and that we ensure that data subject rights are enforceable and upheld. The Company has the below objectives regarding non-EU data transfers: -

- To comply with GDPR Articles 44-50 regarding personal data transfers to a third country or an international organization
- To have adequate and appropriate safeguards and measures in place to protect personal data and data subjects when transferring personal information
- To only transfer data outside the EU where there is an adequacy decision by ***the European Commission*** *(hereinafter referred to as 'the Commission')*, one or more of the appropriate safeguards are place or the transfer complies with one of the transfer exceptions
- To train and support all employees involved in personal data transfers
- To have robust and compliant policies and procedures in place for effecting non-EU transfers
- To regularly review and monitor this policy and any associated procedures

3.5 Guidelines & Procedures

Where data is being transferred for a legal and necessary purpose, compliant with all Articles in the Regulation, we utilize a process that ensures such data is encrypted with a secret key and where possible is also subject to our data minimization methods.

3.5.1 Adequacy Decision

Where we intend to transfer personal data to a third country or an international organization, we check if the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection.

The DPO is responsible for monitoring the approved third country list provided by the Commission and only transferring data under this provision to those countries, organizations or sectors listed.

3.5.2 Appropriate Safeguards

In the absence of a decision by the Commission on an adequate level of protection by a third country or an international organization, we restrict transfers to those that are legally binding or essential for the provision of our business obligations or in the best interests of the data subject. In such instances, we develop and implement appropriate measures and safeguards to protect the data, during transfer and for the duration it is processed and/or stored with the third country or international organization.

3.5.3 Transfer Exceptions

The Company does not transfer any personal information to a third country or international organization without an adequacy decision by the Commission or with Supervisory Authority authorization and the appropriate safeguarding measures; unless one of the below conditions applies. ***The transfer is: -***

- made with the explicit consent of the data subject, after having been informed of the possible risks and the absence of an adequacy decision and appropriate safeguards
- necessary for the performance of a contract between the data subject and the Company or the implementation of pre-contractual measures taken at the data subject's request
- necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the Company and another natural or legal person
- necessary for important reasons of public interest
- necessary for the establishment, exercise or defence of legal claims
- necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent

3.6 Responsibilities

The Data Protection Officer has overall responsibility for reviewing data that is to be transferred to a third country or international.

4. Subject Access Request Procedures

4.1 Introduction

This procedure document supplements the subject access request (SAR) provisions set out in **Integrated Connections, Inc.'s** *(hereinafter referred to as the **"Company"**)* Data Protection Policy & Procedures and provides the process for individuals to use when making an access request, along with the protocols followed by the Company when such a request is received.

The Company needs to collect personal information to effectively and compliantly carry out our everyday business functions and services and in some circumstances, to comply with the requirements of the law and/or regulations.

As the Company processes personal information regarding individuals (*data subjects*), we are obligated under the General Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with the GDPR and its principles.

4.1.1 The General Data Protection Regulation

The General Data Protection Regulation (GDPR) gives individuals the right to know what information is held about them, to access this information and to exercise other rights, including the rectification of inaccurate data. The GDPR is a standardized regulatory framework which ensures that personal information is obtained, handled and disposed of properly.

As the Company are obligated under the GDPR an other data protection laws, we abide by the Regulations' principles, ***which ensure that personal information shall be: -***

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ***('lawfulness, fairness and transparency')***

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ***('purpose limitation')***

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ***('data minimization')***

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ***('accuracy')***

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ***('storage limitation')***

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ***('integrity and confidentiality').***

The Regulation also requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the GDPR principles'* ***('accountability')***. The Company have adequate and effective measures, controls and procedures in place, that protect and secure your personal information and guarantee that it is only ever obtained, processed and disclosed in accordance with the relevant data protection laws and regulations.

4.2 What is Personal Information?

Information protected under the GDPR is known as "personal data" and is defined as: -

"Any information relating to an identified or identifiable natural person; 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."

Further information on what constitutes personal information and your rights under the data protection regulation and laws can be found on the Information Commissioners Office (ICO) **website**.

4.3 The Right of Access

Under Article 15 of the GDPR, an individual has the right to obtain from the controller, confirmation as to whether personal data concerning them is being processed. We are committed to upholding the rights of individuals and have dedicated processes in place for providing access to personal information. ***Where requested, we will provide the following information: -***

- the purposes of the processing
- the categories of personal data concerned
- the recipient(s) or categories of recipient(s) to whom the personal data have been or will be disclosed
- If the data has been transferred to a third country or international organization(s) (*and if applicable, the appropriate safeguards used)*
- the envisaged period for which the personal data will be stored (*or the criteria used to determine that period)*

- where the personal data was not collected directly from the individual, any available information as to its source

4.3.1 How To Make a SAR?

A subject access request (SAR) is a request for access to the personal information that the Company holds about you, which we are required to provide under the GDPR *(unless an exemption applies*). The information that we provide is covered in section 3 of this document.

You can make this request in writing using the details provided in section 0, or you can submit your access request electronically. Where a request is received by electronic means, we will provide the requested information in a commonly used electronic form *(unless otherwise requested by the data subject).*

4.3.2 What We Do When We Receive An Access Request

Identity Verification

Subject Access Requests (SAR) are passed to the **Data Protection Officer** as soon as received and a record of the request is made. The person in charge will use all reasonable measures to verify the identity of the individual making the access request, especially where the request is made using online services.

We will utilize the request information to ensure that we can verify your identity and where we are unable to do so, we may contact you for further information, or ask you to provide evidence of your identity prior to actioning any request. This is to protect your information and rights.

If a third party, relative or representative is requesting the information on your behalf, we will verify their authority to act for you and again, may contact you to confirm their identity and gain your authorization prior to actioning the any request.

Information Gathering

If you have provided enough information in your SAR to collate the personal information held about you, we will gather all documents relating to you and ensure that the information required is provided in an acceptable format. If we do not have enough information to locate your records, we may contact you for further details. This will be done as soon as possible and within the timeframes set out below.

Information Provision

Once we have collated all the personal information held about you, we will send this to you in writing (*or in a commonly used electronic form if requested*). The information will be in a concise, transparent, intelligible and easily accessible format, using clear and plain language.

4.4 Fees and Timeframes

We aim to complete all access requests within 30-days and provide the information free of charge. Where the request is made by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested.

While we provide the information requested without a fee, further copies requested by the individual may incur a charge to cover our administrative costs.

The Company always aim to provide the requested information at the earliest convenience, but at a maximum, 30 days from the date the request is received. However, where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months. If this is the case, we will write to you within 30 days and keep you informed of the delay and provide the reasons.

4.5 Your Other Rights

Under the GDPR, you have the right to request rectification of any inaccurate data held by us. Where we are notified of inaccurate data, and agree that the data is incorrect, we will amend the details immediately as directed by you and make a note on the system *(or record)* of the change and reason(s).

We will rectify any errors within 30-days and inform you in writing of the correction and where applicable, provide the details of any third-party to whom the data has been disclosed.

If for any reason, we are unable to act in response to a request for rectification and/or data completion, we will always provide a written explanation to you and inform you of your right to complain to the Supervisory Authority and to seek a judicial remedy.

In certain circumstances, you may also have the right to request from the Company, the erasure of personal data or to restrict the processing of personal data where it concerns your personal information; as well as the right to object to such processing. You can use the contact details in section 7 to make such requests.

4.6 Exemptions and Refusals

The GDPR contains certain exemptions from the provision of personal information. If one or more of these exemptions applies to your subject access request or where the Company does not act upon the request, we shall inform you at the earliest convenience, or at the latest, within one month of receipt of the request.

Where possible, we will provide you with the reasons for not acting and any possibility of lodging a complaint with the Supervisory Authority and your right to seek a judicial remedy. Details of how to contact the Supervisory Authority are laid out in section 7 of this document.

4.7 Submission & Lodging a Complaint

To submit your SAR, you can contact us at lisam@integratedconnects.com. You can also submit your request in writing using the ***form in Appendix 1***, sending the request to: -
DPO: 301 S Howes, #2315, Fort Collins, CO USA 80522

4.7.1 Representation for data subjects in the EU

We value your privacy and your rights as a data subject and have therefore appointed Prighter as our privacy representative and your point of contact.

Prighter gives you an easy way to exercise your privacy-related rights (e.g. requests to access or erase personal data). If you want to contact us via our representative Prighter or make use of your data subject rights, please visit: https://prighter.com/q/11664981086

4.7.2 Supervisory Authority

If you remain dissatisfied with our actions, you have the right to lodge a complaint with the Supervisory Authority. ***The Information Commissioner's Office (ICO) can be contacted at: -***

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: 0303 123 1113 *(local rate)* or 01625 545 745 *(national rate)*
Fax: 01625 524 510
Email: enquiries@ico.org.uk

Subject Access Request Form

Under the General Data Protection Regulation, you are entitled as a data subject to obtain from the Company, confirmation as to whether we are processing personal data concerning you, as well as to request details about the purposes, categories and disclosure of such data.

You can use this form to request information about, and access to any personal data we hold about you. Details on where to return the completed form can be found at the end of the document.

1. Personal Details:

Data Subject's Name:		**DOB:**	___ / ___ / _____
Home Telephone No:		**Email:**	

Data Subject's Address:

Any other information that may help us to locate your personal data:

2. Specific Details of the Information Requested:

3. Representatives *(only complete if you are acting as the representative for a data subject)*
***[Please Note:** We may still need to contact the data subject where proof of authorization or identity are required]*

Representative's Name:		**Relationship to Data Subject:**	
Telephone No:		**Email:**	

Representative's Address:

I confirm that I am the authorized representative of the named data subject:

Representative's Name: **Signature:** _____

_____

4. Confirmation

Data Subject's Name: _____ [print name]

Signature: _____ **Date:** ____ /____ /_____

5. Completed Forms

For postal requests, please return this form to:
DPO: 301 S. Howes, # 2315, Fort Collins, CO USA 80522

For email requests, please return this form to: General Counsel at lisam@integratedconnects.com

5. Data Breach Policy and Procedures

5.1 Policy Statement

Integrated Connections, Inc. *(hereinafter referred to as the **"Company"**)* are committed to our obligations under the regulatory system and in accordance with the GDPR and maintain a robust and structured program for compliance and monitoring. However, we recognize that breaches can occur, hence this policy states our intent and objectives for dealing with such incidents.

Although we understand that not all risks can be mitigated, we operate a robust and structured system of controls, measures and processes to help protect data subjects and their personal information from any risks associated with processing data. The protection and security of the personal data that we process is of paramount importance to us and we have developed data specific protocols for any breaches relating to the GDPR and the data protection laws.

5.2 Purpose

The purpose of this policy is to provide the Company's intent, objectives and procedures regarding data breaches involving personal information. As we have obligations under the GDPR, we also have a requirement to ensure that adequate procedures, controls and measures are in place and are disseminated to all employees; ensuring that they are aware of the protocols and reporting lines for data breaches. This policy details our processes for reporting, communicating and investigating such breaches and incidents.

5.3 Scope

This policy applies to all staff within the Company *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the US or overseas).* Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

5.4 Data Security & Breach Requirements

The Company's definition of a personal data breach is any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

Alongside our *'Privacy by Design'* approach to protecting data, we also have a legal, regulatory and business obligation to ensure that personal information is protected while being processed by the Company. Our technical and organizational measures are detailed in our Data Protection Policy Procedures, Chapter 1.

5.4.1 Objectives

- To adhere to the GDPR laws and to have robust and adequate procedures and

controls in place for identifying, investigating, reporting and recording any data breaches

- To develop and implement adequate, effective and appropriate technical and organizational measures to ensure a high level of security with regards to personal information
- To utilize information audits and risk assessments for mapping data and to reduce the risk of breaches
- To have adequate and effective risk management procedures for assessing any risks presented by processing personal information
- To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes set out in any regulations, codes of practice or handbooks
- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring
- To use the Data Breach Incident Form for all data breaches, regardless of severity so that any patterns in causes can be identified and corrected
- To protect consumers, clients and employees; including their information and identity
- To ensure that where applicable, the Data Protection Officer (the "DPO") is involved in and notified about all data breaches and risk issues
- To ensure that the Supervisory Authority is notified of any data breach (*where applicable*) with immediate effect and at the latest, within 72 hours of the Company having become aware of the breach

5.5 Data Breach Procedures & Guidelines

The Company has robust objectives and controls in place for preventing data breaches and for managing them in the rare event that they do occur. Our procedures and guidelines for identifying, investigating and notification of breaches are detailed below. Our documented breach incident policy aims to mitigate the impact of any data breaches and to ensure that the correct notifications are made.

5.5.1 Breach Monitoring & Reporting

The Company has appointed a **Data Protection Officer** who is responsible for the review and investigation of any data breach involving personal information, regardless of the severity, impact or containment. All data breaches are reported to this person with immediate effect, whereby the procedures detailed in this policy are followed.

All data breaches will be investigated, even in instances where notifications and reporting are not required, and we retain a full record of all data breaches to ensure that gap and pattern analysis are available and used. Where a system or process failure has given rise to

a data breach, revision to any such process is recorded in the Change Management and Document Control records.

1.5.2 Breach Incident Procedures

5.5.2.1 Identification of an Incident

As soon as a data breach has been identified, it is reported to the direct line manager and the reporting officer *Data Protection Officer* immediately so that breach procedures can be initiated and followed without delay.

Reporting incidents in full and with immediate effect is essential to the compliant functioning of the Company and is not about apportioning blame. These procedures are for the protection of the Company, its staff, customers, clients and third parties and are of the utmost importance for legal regulatory compliance.

As soon as an incident has been reported, measures must be taken to contain the breach. Such measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken; however, the aim of any such measures should be to stop any further risk/breach to the organization, customer, client, third-party, system or data prior to investigation and reporting. The measures taken are noted on the incident form in all cases.

5.5.2.2 Breach Recording

The Company utilizes a Breach Incident Form for all incidents, which is completed for any data breach, regardless of severity or outcome. Completed forms are logged in the Breach Incident Folder *(electronic or hard-copy)* and reviewed against existing records to ascertain patterns or reoccurrences.

In cases of data breaches, the **Data Protection Officer** is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, recording the incident on the breach form and making any relevant and legal notifications. The completing of the Breach Incident Form is only to be actioned after containment has been achieved.

A full investigation is conducted and recorded on the incident form, with the outcome being communicated to all staff involved in the breach, in addition to senior management. A copy of the completed incident form is filed for audit and documentation purposes.

If applicable, the Supervisory Authority and the data subject(s) are notified in accordance with the GDPR requirements. The Supervisory Authority protocols are to be followed and their '***Security Breach Notification Form'*** should be completed and submitted. In addition, any individual whose data or personal information has been compromised is

notified if required, and kept informed throughout the investigation, with a full report being provided of all outcomes and actions.

5.5.3 Breach Risk Assessment

5.5.3.1 Human Error

Where the data breach is the result of human error, an investigation into the root cause is to be conducted and a formal interview with the employee(s) held.

A review of the procedure(s) associated with the breach is conducted and a full risk assessment completed in accordance with the Company's Risk Assessment Procedures. Any identified gaps that are found to have caused/contributed to the breach are revised and risk assessed to mitigate any future occurrence of the same root cause.

Resultant employee outcomes of such an investigation can include, but are not limited to: -

- Re-training in specific/all compliance areas
- Re-assessment of compliance knowledge and understanding
- Suspension from compliance related tasks
- Formal warning *(in-line with the Company's disciplinary procedures)*

5.5.3.2 System Error

Where the data breach is the result of a system error/failure, the IT team are to work in conjunction with the **DPO** to assess the risk and investigate the root cause of the breach. A gap analysis is to be completed on the system/s involved and a full review and report to be added to the Breach Incident Form.

Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause. Full details of the incident should be determined and mitigating action such as the following should be taken to limit the impact of the incident: -

- Attempting to recover any lost equipment or personal information
- Shutting down an IT system
- Removing an employee from their tasks
- The use of back-ups to restore lost, damaged or stolen information
- Making the building secure
- If the incident involves any entry codes or passwords, then these codes must be changed immediately and members of staff informed

5.5.3.3 Assessment of Risk and Investigation

The **DPO** should ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches.

The lead investigator should look at: -

- The type of information involved
- It's sensitivity or personal content
- What protections are in place (e.*g. encryption*)?
- What happened to the information/Where is it now?
- Whether there are any wider consequences/implications to the incident

The appointed lead should keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions.

5.6 Breach Notifications

The Company recognizes our obligation and duty to report data breaches in certain instances. All staff have been made aware of the Company's responsibilities and we have developed strict internal reporting lines to ensure that data breaches falling within the notification criteria are identified and reported without delay.

5.6.1 Supervisory Authority Notification

The Supervisory Authority is to be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, would lead to significant detrimental effects on the individual.

Where applicable, the Supervisory Authority is notified of the breach no later than 72 hours after the Company becoming aware of it and are kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes.

If for any reason it is not possible to notify the Supervisory Authority of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay. Where a breach is assessed by the DPO and deemed to be ***unlikely*** to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Supervisory Authority in accordance with Article 33 of the GDPR.

The notification to the Supervisory Authority will contain: -

- A description of the nature of the personal data breach

- The categories and approximate number of data subjects affected
- The categories and approximate number of personal data records concerned
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (*for obtaining further information)*
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach *(including measures to mitigate its possible adverse effects)*

Breach incident procedures should be followed and an investigation carried out, regardless of our notification obligations and outcomes, with reports being retained and made available to the Supervisory Authority if requested.

Where the Company acts in the capacity of a processor, we will ensure that controller is notified of the breach without undue delay. In instances where we act in the capacity of a controller using an external processor, we have a written agreement in place to state that the processor is obligated to notify us without delay after becoming aware of a personal data breach.

5.6.2 Data Subject Notification

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written, clear and legible format.

The notification to the Data Subject shall include: -

- The nature of the personal data breach
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (*for obtaining further information)*
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach *(including measures to mitigate its possible adverse effects)*

We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organizational measures which render the data unintelligible to any person who is not authorized to access it *(i.e. encryption, data masking etc*) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialize.

If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

5.7 Record Keeping

All records and notes taking during the identification, assessment and investigation of the data breach are recorded and authorized by the **Data Protection Officer** and are retained for a period of 6 years from the date of the incident. Incident forms are to be reviewed monthly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

5.8 Responsibilities

The Company will ensure that all staff are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as understanding their responsibilities and the breach incident reporting lines.

The **Data Protection Officer** is responsible for regular compliance audits and gap analysis monitoring and the subsequent reviews and action follow ups. There is a continuous audit trail of all compliance reviews and procedural amendments and feedback to ensure continuity through each process and task.

6. Data Breach Incident Form

DPO/COMPLIANCE OFFICER/INVESTIGATOR DETAILS:			
NAME:		**POSITION:**	
DATE:		**TIME:**	
TEL:		**EMAIL:**	
INCIDENT INFORMATION:			
DATE/TIME OR PERIOD OF BREACH:			
DESCRIPTION & NATURE OF BREACH:			
TYPE OF BREACH:			

CATEGORIES OF DATA SUBJECTS AFFECTED:			
CATEGORIES OF PERSONAL DATA RECORDS CONCERNED:			
NO. OF DATA SUBJECTS AFFECTED:		**NO. OF RECORDS INVOLVED:**	
IMMEDIATE ACTION TAKEN TO CONTAIN/MITIGATE BREACH:			
STAFF INVOLVED IN BREACH:			
PROCEDURES INVOLVED IN BREACH:			
THIRD PARTIES INVOLVED IN BREACH:			
BREACH NOTIFICATIONS:			
WAS THE SUPERVISORY AUTHORITY NOTIFIED?		**YES/NO**	
IF YES, WAS THIS WITHIN 72 HOURS?		**YES/NO/NA**	
If no to the above, provide reason(s) for delay			

WAS THE BELOW INFORMATION PROVIDED? *(if applicable)*	**YES**	**NO**
A description of the nature of the personal data breach		
The categories and approximate number of data subjects affected		
The categories and approximate number of personal data records concerned		
The name and contact details of the Data Protection Officer and/or any other relevant point of contact (for obtaining further information)		

A description of the likely consequences of the personal data breach		
A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)		
WAS NOTIFICATION PROVIDED TO DATA SUBJECT?	**YES/NO**	
INVESTIGATION INFORMATION & OUTCOME ACTIONS:		
DETAILS OF INCIDENT INVESTIGATION:		
PROCEDURE(S) REVISED DUE TO BREACH:		
STAFF TRAINING PROVIDED: *(if applicable)*		
DETAILS OF ACTIONS TAKEN AND INVESTIGATION OUTCOMES:		
HAVE THE MITIGATING ACTIONS PREVENTED THE BREACH FROM OCCURRING AGAIN? *(Describe)*		
WERE APPROPRIATE TECHNICAL MEASURES IN PLACE?	**YES/NO**	
If yes to the above, describe measures		

Investigator Signature: _____ Date: _____ Investigator Name: _____ Authorized by: _____