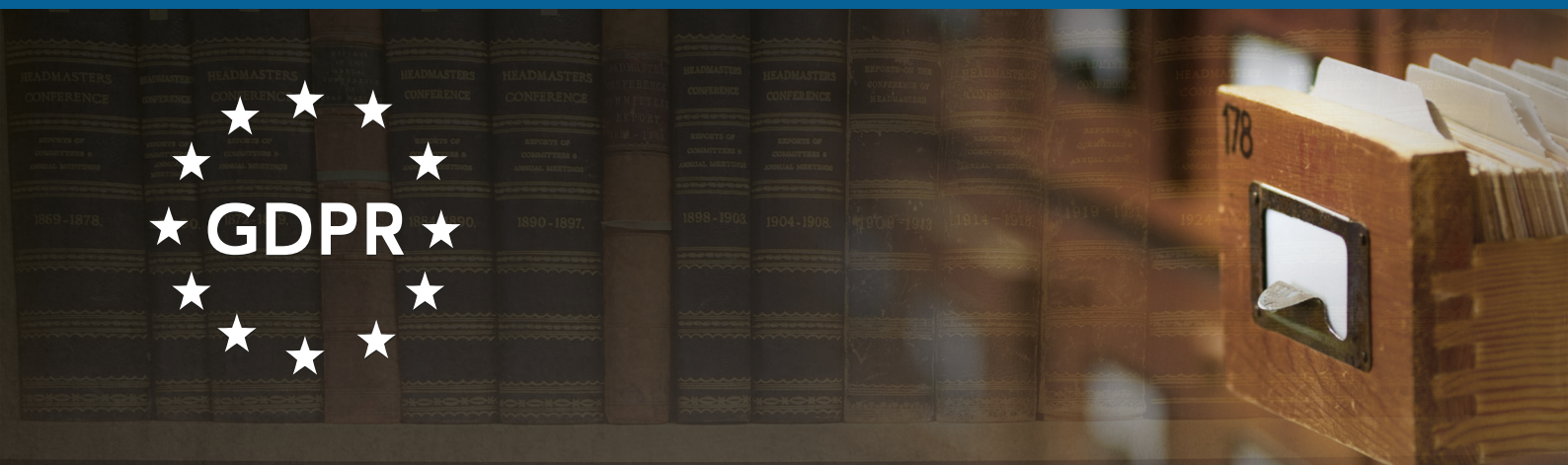
sds group

GDPR Policy Manual



Specialists in Managing School **Archives**

SCANNING, INDEXING AND DOCUMENT MANAGEMENT EXPERTS

Records Management
Heritage Archives
Estates & O&Ms
Admin Records
HR & Personnel

Finance & Accounts
Photographs
Admissions
Pupil Leaver's Files
Policy & Procedures

Audits & Inspections
School Registers
Journals and Publications
Governor's Minutes
Certification & Compliance

- We maintain that privacy and data protection for all Clients are part of their human rights
- SDS has a duty of care to the people within our data storage
- Data is a liability; it should only be collected and processed when absolutely necessary
- SDS never sell, rent or otherwise distribute or make public your personal information except as part of the contract

SDS Group Hello House, 135 Somerford Road, Christchurch, Dorset, BH23 3PY

GDPR Statement – SDS Group

General Data Protection Regulation (GDPR)

Introduction

The new European Union General Data Protection Regulation (EU GDPR) will come into effect in the UK from 25th May 2018. The new Regulation enhances the safeguards for individuals in the existing Data Protection Act which will also be replaced with a new UK Data Protection Bill in 2018. SDS Group is committed to high standards of information security, privacy and transparency. We place a high priority on protecting and managing. The company will comply with applicable GDPR regulations when they take effect in 2018, including as a data processor, while also working closely with our clients and partners to meet contractual obligations for our procedures, products and services.

The Regulation gives individuals the right to ask businesses for detailed information about how their "Personally Identifiable Information (PII)" is stored and processed. In the Regulation there is no distinction between personal data about individuals in their private, public or work roles.

1. Compliance

SDS Group has always taken the security of information very seriously and has introduced systems to help ensure that it processes any PII securely and in accordance with all applicable regulatory and legislative requirements. This Policy sets out our objective of meeting these requirements in a logical method.

2. SDS Group websites and web-based applications

SDS Group offers a range of web and web-based applications and as such the company is committed to providing technology solutions to support customers' GDPR obligations.

Our IT infrastructure is rigorously and regularly SOAK & Stress tested for :

- Security
- Data Integrity
- Performance
- Control and Audit
- Back-up and Resilience
- Risk

SDS ensure that where clients' data which is sensitive, or falls within the parameters of the GDPR regulations, that only London UK Cloud based servers are used (this way we can guarantee that your data will never find its way onto a European, USA or Worldwide Cloud based set-up).

3. SDS Group and Data we may hold

SDS Group as a company holds very little relevant Data. That which we do hold is not financial and only minimal personal data for archiving purposes (please see Data Protection Bill -GDPR (Archiving Section -P138, part 6, para 26, section 1).

However, all Data we hold is on our private Servers drives, and that is stored behind a secure SSL. This provides encrypted security.

SDS retains no rights of ownership of any data which we scan or process for our clients. All copyrights and proprietorships remain with our clients. Our clients can have all their data returned to them at requested without any penalty or forfeit.

Mark Coleman SDS Group Managing Director

CONTENTS

APPROVAL AND REVIEW DETAILS

Approval and Review	**Details**
Approval Authority	Managing Director & Data Protection Officer
Data Protection Officer	Chave Anderson
Next Review Date	01/05/2021

Approval and Amendment History	**Details**
Original Approval Authority and Date	Mark Coleman Managing Director 01/05/2018
Amendment Authority and Date	Draft: Managing Director 24/04/2018
	Review: Managing Director 27/04/2018
	Audit/Approval: Managing Director 01/05/2018
	Final: Managing Director 15/05/2018

DATA PROTECTION POLICY

CONTENTS

1 PURPOSE

This policy establishes an effective, accountable and transparent framework for ensuring compliance with the requirements of the GDPR.

2 SCOPE

This policy applies to all SDS Group employees and all third parties responsible for the processing of personal data on behalf of SDS Group services/entities.

3 POLICY STATEMENT

SDS Group is committed to conducting its business in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of SDS Group employees and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to a SDS Group contact (i.e. the data subject).

Personal data is any information (including opinions and intentions) which relates to an identified or identifiable natural person. Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data. An organisation that handles personal data and makes decisions about its use is known as a Data Controller. SDS Group, as a Data Controller, is responsible for ensuring compliance with the data protection requirements outlined in this policy. Non-compliance may expose SDS Group to complaints, regulatory action, fines and/or reputational damage.

SDS Group's leadership is fully committed to ensuring continued and effective implementation of this policy, and expects all SDS Group employees and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

3.1. Governance

3.1.1. Data Protection Officer

To demonstrate our commitment to data protection, and to enhance the effectiveness of our compliance efforts, SDS Group has appointed a Data Protection Officer. The Data Protection Officer operates with independence and is supported by suitability skilled individuals granted all necessary authority. The Data Protection Officer's duties include:

- Informing and advising SDS Group and its employees who carry out processing pursuant to data protection regulations, national law or European Union based data protection provisions;
- Ensuring the alignment of this policy with data protection regulations, national law or European Union based data protection provisions;
- Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);
- Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs);
- Determining the need for notifications to one or more DPAs as a result of SDS Group's current or intended personal data processing activities;
- Making and keeping current notifications to one or more DPAs as a result of SDS Group's current or intended personal data processing activities;
- The establishment and operation of a system providing prompt and appropriate responses to data subject requests;
- Informing senior managers, officers, and directors of SDS Group of any potential corporate, civil and criminal penalties which may be levied against SDS Group and/or its employees for violation of applicable data protection laws.

Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any third party who:

- provides personal data to a SDS Group service/entity
- receives personal data from a SDS Group service/entity
- has access to personal data collected or processed by a SDS Group

3.1.2. Data Protection by Design

To ensure that all data protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing. Each SDS Group service/entity must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Data Protection Officer, for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the CEO for review and approval. Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will cooperate with the Data Protection Officer to assess the impact of any new technology uses on the security of personal data.

3.1.3. Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by all SDS Group services/entities in relation to this policy, the Data Protection Officer will carry out an annual data protection compliance audit for all such services/entities. Each audit will, as a minimum, assess:

- Compliance with policy in relation to the protection of personal data, including:
- The assignment of responsibilities.
  - ü Raising awareness.
  - ü Training of employees.
- The effectiveness of data protection related operational practices, including:
  - ü Data subject rights.
  - ü Personal data transfers.
  - ü Personal data incident management.
  - ü Personal data complaints handling.
  - ü The level of understanding of data protection policies and privacy notices.
  - ü The currency of data protection policies and privacy notices.
  - ü The accuracy of personal data being stored.
  - ü The conformity of data processor activities.
  - ü The adequacy of procedures for redressing poor compliance and personal data breaches. The Data Protection Officer, in cooperation with key business stakeholders from each SDS Group service/entity, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies and good practice identified will be reported to, monitored and shared by the SDS Group Managing Director.

3.2. Data Protection Principles

SDS Group has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data:

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

Principle 2: Purpose Limitation. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means SDS Group must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means SDS Group must not store any personal data beyond what is strictly required.

Principle 4: Accuracy. Personal data shall be accurate and, kept up to date. This means SDS Group must have in place processes for identifying and addressing out-of-date, incorrect and redundant personal data.

Principle 5: Storage Limitation. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. This means SDS Group must, wherever possible, store personal data in a way that limits or prevents identification of the data subject.

Principle 6: Integrity & Confidentiality. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. SDS Group must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

Principle 7: Accountability. The Data Controller shall be responsible for, and be able to demonstrate compliance. This means SDS Group must demonstrate that the six data protection principles (outlined above) are met for all personal data for which it is responsible.

3.3. Data collection

3.3.1. Data Sources

Personal data should be collected only from the data subject unless one of the following apply:

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

If personal data is collected from someone other than the data subject, the data subject must be informed of the collection unless one of the following apply:

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

Where it has been determined that notification to a data subject is required, notification should occur promptly, but in no case later than:

- Two calendar months from the first collection or recording of the personal data
- At the time of first communication if used for communication with the data subject
- At the time of disclosure if disclosed to another recipient.

3.3.2. Data subject consent

Each SDS Group service/entity will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, SDS Group is committed to seeking such consent. The Data Protection Officer, in cooperation with other relevant business representatives, shall establish a system for obtaining and documenting data subject consent for the collection, processing, and/or transfer of their personal data.

3.3.3. Data subject Notification

Each SDS Group service/entity will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide data subjects with information as to the purpose of the processing of their personal data. When the data subject is asked to give consent to the processing of personal data and when any personal data is collected from the data subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The data subject already has the information;
- A legal exemption applies to the requirements for disclosure and/or consent. The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Data Protection Officer. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

3.3.4. External Privacy Notices

Each external website provided by SDS Group will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law.

3.4. Data Use

3.4.1. Data processing

SDS Group uses the personal data of its contacts for the following broad purposes:

- The general running and business administration of SDS Group services/entities.
- To provide services to SDS Group's stakeholders.
- The ongoing administration and management of customer services.

The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a contact's expectations that their details will be used by SDS Group to respond to a contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that SDS Group would then provide their details to third parties for marketing purposes.

Each SDS Group service/entity will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, SDS Group will not process personal data unless at least one of the following requirements are met:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child).

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

- In any circumstance where consent has not been gained for the specific processing in question, SDS Group will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the personal data was collected: Any link between the purpose for which the personal data was collected and the reasons for intended further processing.

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

3.4.2. Special Categories of Data

SDS Group will only process special categories of data (also known as sensitive data) where the data subject expressly consents to such processing or where one of the following conditions apply:

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

In any situation where special categories of data are to be processed, prior approval must be obtained from the Data Protection Officer, and the basis for the processing clearly recorded with the personal data in question. Where special categories of data are being processed, SDS Group will adopt additional protection measures.

3.4.3. Children's Data

Children under the age of 14 are unable to consent to the processing of personal data for information society services (any service normally provided for payment, by electronic means and at the individual request of a recipient of services). Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

3.4.4. Data Quality

Each SDS Group service/entity will adopt all necessary measures to ensure that the personal data it collects and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the data subject. The measures adopted by SDS Group to ensure data quality include:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification.
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required.
- Restriction, rather than deletion of personal data, insofar as:
    - **ü** a law prohibits erasure.
    - **ü** erasure would impair legitimate interests of the data subject.
    - **ü** the data subject disputes that their personal data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

3.4.5. Profiling & Automated Decision Making

SDS Group will only engage in profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the data subject or where it is authorised by law. Where an SDS Group

service/entity utilises profiling and automated decision-making, this will be disclosed to the relevant data subjects. In such cases the data subject will be given the opportunity to:

- Express their point of view.
- Obtain an explanation for the automated decision.
- Review the logic used by the automated system.
- Supplement the automated system with additional data.
- Have a human carry out a review of the automated decision.
- Contest the automated decision.

Object to the automated decision-making being carried out. Each SDS Group service/entity must also ensure that all profiling and automated decision-making relating to a data subject is based on accurate data.

3.4.6. Digital Marketing

As a general rule SDS Group will not send promotional or direct marketing material to an SDS Group Contact through digital channels such as mobile phones, email and the Internet, without first obtaining their consent. Any SDS Group service/entity wishing to carry out a digital marketing campaign without obtaining prior Consent from the data subject must first have it approved by the Data Protection Officer. Where personal data processing is approved for digital marketing purposes, the data subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data processed for such purposes. If the data subject puts forward an objection, digital marketing related processing of their personal data must cease immediately and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted. It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

3.5. Data Retention

To ensure fair processing, personal data will not be retained by SDS Group for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which SDS Group services/entities need to retain personal data is set out in SDS Group '*Data Retention Policy'*. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

3.6. Data Protection

Each SDS Group service/entity will adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of the personal data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data are processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes can and is processed separately.
- Ensure that personal data is not kept longer than necessary

3.7. Data subject Requests

The Data Protection Officer will establish a system to enable and facilitate the exercise of data subject rights related to:

- Information access.
- Objection to processing.
- Objection to automated decision-making and profiling.
- Restriction of processing.
- Data portability.
- Data rectification.
- Data erasure. If an individual makes a request relating to any of the rights listed above

SDS Group will consider each such request in accordance with all applicable data protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature. data subjects are entitled to obtain, based upon a request made in writing/email to: gdpr@sds-group.co.uk.

It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights. Detailed guidance for dealing with requests from data subjects can be found in SDS Group's '*Data Subject Access Rights Policy and Procedure*' document.

3.8. Law Enforcement Requests & Disclosures

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

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

If an SDS Group service/entity processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. If any SDS Group service/entity receives a request from a court or any regulatory or law enforcement authority for information relating to an SDS Group contact, you must immediately notify the Data Protection Officer who will provide comprehensive guidance and assistance.

3.9. Data Protection Training

All SDS Group employees that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, each SDS Group service/entity will provide regular Data Protection training and procedural guidance for their staff.

3.10. Data Transfers

SDS Group services/entities may transfer personal data to internal or third party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. third countries), they must be made in compliance with an approved transfer mechanism. SDS Group services/entities may only transfer personal data where one of the transfer scenarios list below applies:

- The data subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the data subject

- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject

3.11. Complaints handling

Data subjects with a complaint about the processing of their personal data, should put forward the matter in writing to the Data Protection Officer. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Officer will inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the data subject and the Data Protection Officer, then the data subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

3.12. Breach Reporting

Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data must immediately notify the Data Protection Officer providing a description of what occurred. Notification of the incident can be made via e-mail, by calling, or by contacting the Information Commissioner's Office (ICO) ico.org.uk. The Data Protection Officer will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Data Protection Officer will follow the relevant authorised procedure based on the criticality and quantity of the personal data involved. For severe personal data breaches, SDS Group Managing Director will initiate and chair an emergency response team to coordinate and manage the personal data breach response.

4 ROLES AND RESPONSIBILITIES

4.1 Implementation

The management team of each SDS Group service/entity must ensure that all SDS Group employees responsible for the processing of personal data are aware of and comply with the contents of this policy. In addition, each SDS Group service/entity will make sure all third parties engaged to process personal data on their behalf (i.e. their data processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all third parties, whether companies or individuals, prior to granting them access to personal data controlled by SDS Group.

4.2 Support, Advice and Communication

For advice and support in relation to this policy, please contact the Data Protection Officer email gdpr@sds-group.co.uk.

5 REVIEW

This policy will be reviewed by the Data Protection Officer every three years, unless there are any changes to regulations or legislation that would enable a review earlier.

6 RECORDS MANAGEMENT

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised SDS Group recordkeeping system.

All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

7 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and

the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data.

Data Processor: the entity that processes data on behalf of the Data Controller.

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union.

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

Data subject: a natural person whose personal data is processed by a controller or processor.

personal data: any information related to a natural person or 'data subject', that can be used to directly or indirectly identify the person.

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data.

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.

Regulation: a binding legislative act that must be applied in its entirety across the Union.

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

8 RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Information Commissioner's Office Certificate of Registration Number Z2451889

9 FEEDBACK AND SUGGESTIONS

SDS Group employees may provide feedback and suggestions about this document by emailing mark@sds-group.co.uk.

10 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Managing Director & Data Protection Officer
Data Protection Officer	Chave Anderson
Next Review Date	01/05/2021

Approval and Amendment History	Details
Original Approval Authority and Date	Mark Coleman Managing Director 01/05/2018
Amendment Authority and Date	Draft: Managing Director 24/04/2018
	Review: Managing Director 27/04/2018
	Audit/Approval: Managing Director 01/05/2018
	Final: Managing Director 15/05/2018

Privacy Notice

Introduction

This document refers to personal data, which is defined as information concerning any living person (a natural person who hereafter will be called the Data Subject) that is not already in the public domain.

The General Data Protection Regulation (GDPR) seeks to protect and enhance the rights of data subjects. These rights cover the safeguarding of personal data, protection against the unlawful processing of personal data and the unrestricted movement of personal data within the EU. It should be noted that GDPR does not apply to information already in the public domain.

SDS Group is pleased to provide the following Privacy Notice:

Personal Data

SDS Group uses the information collected from you to provide quotations, make telephone contact and to email you marketing information which SDS Group believes may be of interest to you and your business. In you making initial contact you consent to SDS Group maintaining a marketing dialogue with you until you either opt out (which you can do at any stage) or we decide to desist in promoting our services. SDS Group also acts on behalf of its clients in the capacity of data processor. When working exclusively as a data processor, SDS Group will be acting on the instruction of its client, and will work hard to ensure that the client is fully GDPR compliant.

Some personal data may be collected about you from the forms and surveys you complete, from records of our correspondence and phone calls and details of your visits to our website, including but not limited to personally identifying information like Internet Protocol (IP) addresses. SDS Group may from time to time use such information to identify its visitors. SDS Group may also collect statistics about the behavior of visitors to its website.

SDS Group's websites uses cookies, which is a string of information that a website stores on a visitor's computer, and that the visitor's browser provides to the website each time the visitor returns. WordPress.org uses cookies to help SDS Group identify and track visitors and their website access preferences. SDS Group website visitors who do not wish to have cookies placed on their computers should set their browsers to refuse cookies before using SDS Group' website.

Any information SDS Group holds about you and your business encompasses all the details we hold about you and any sales transactions including any third-party information we have obtained about you from public sources and our own suppliers such as credit referencing agencies.

SDS Group will only collect the information needed so that it can provide you with marketing and consulting services, this agency does not sell or broker your data, although coincidentally there may be times when your information could be contained in data that SDS Group has purchased from a third-party list broker, on behalf of a client.

Legal basis for processing any personal data

To meet SDS Group' contractual obligations to clients and to also respond to marketing enquiries.

Legitimate interests pursued by SDS Group and/or its clients

To promote the marketing and consulting services offered by SDS Group and/or to market the services and/or products offered by SDS Group's existing clients.

Consent

Through agreeing to this privacy notice you are consenting to SDS Group processing your personal data for the purposes outlined. You can withdraw consent at any time by emailing mark@sds-group.co.uk or writing to us, see last section for full contact details.

Disclosure

SDS Group may on occasions pass your Personal Information to third parties exclusively to process work on its behalf. SDS Group requires these parties to agree to process this information based on our instructions and requirements consistent with this Privacy Notice and GDPR.

SDS Group do not broker or pass on information gained from your engagement with the agency without your consent. However, SDS Group may disclose your Personal Information to meet legal obligations, regulations or valid governmental request. The agency may also enforce its Terms and Conditions, including investigating potential violations of its Terms and Conditions to detect, prevent or mitigate fraud or security or technical issues; or to protect against imminent harm to the rights, property or safety of SDS Group, its clients and/or the wider community.

Retention Policy

SDS Group will process personal data during the duration of any contract and will continue to store only the personal data needed for five years after the contract has expired to meet any legal obligations. After five years any personal data not needed will be deleted.

Data storage

Data is held in United Kingdom using different (multiple) servers. SDS Group does not store personal data outside the EEA.

Your rights as a data subject

At any point whilst SDS Group is in possession of or processing your personal data, all data subjects have the following rights:

- Right of access – you have the right to request a copy of the information that we hold about you.
- Right of rectification – you have a right to correct data that we hold about you that is inaccurate or incomplete.
- Right to be forgotten – in certain circumstances you can ask for the data we hold about you to be erased from our records.
- Right to restriction of processing – where certain conditions apply you have a right to restrict the processing.
- Right of portability – you have the right to have the data we hold about you transferred to another organisation.

- Right to object – you have the right to object to certain types of processing such as direct marketing.
- Right to object to automated processing, including profiling – you also have the right not to be subject to the legal effects of automated processing or profiling.

In the event that SDS Group refuses your request under rights of access, we will provide you with a reason as to why, which you have the right to legally challenge.

SDS Group at your request can confirm what information it holds about you and how it is processed

You can request the following information:

- Identity and the contact details of the person or organisation (SDS Group) that has determined how and why to process your data.
- Contact details of the data protection officer, where applicable.
- The purpose of the processing as well as the legal basis for processing.
- If the processing is based on the legitimate interests of SDS Group or a third party such as one of its clients, information about those interests.
- The categories of personal data collected, stored and processed.
- Recipient(s) or categories of recipients that the data is/will be disclosed to.
- How long the data will be stored.
- Details of your rights to correct, erase, restrict or object to such processing.
- Information about your right to withdraw consent at any time.
- How to lodge a complaint with the supervisory authority (Data Protection Regulator).
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether you are obliged to provide the personal data and the possible consequences of failing to provide such data.
- The source of personal data if it wasn't collected directly from you.
- Any details and information of automated decision making, such as profiling, and any meaningful information about the logic involved, as well as the significance and expected consequences of such processing.

To access what personal data is held, identification will be required

SDS Group will accept the following forms of ID when information on your personal data is requested: a copy of your national ID card, driving license, passport, birth certificate and a utility bill not older than three months. A minimum of one piece of photographic ID listed above and a supporting document is required. If SDS Group is dissatisfied with the quality, further information may be sought before personal data can be released.

All requests should be made to gdpr@sds-group.co.uk or by phoning +01425621262 or writing to us at the address further below.

Complaints

In the event that you wish to make a compliant about how your personal data is being processed by SDS Group or its partners, you have the right to complain to SDS Group's CEO. If you do not get a response within 30 days you can complain to the Data Protection Regulator.

The details for each of these contacts are:

SDS Group, attention of the Managing Director
SDS Group
Hello House
135 Somerford Road
Christchurch
Dorset
BH23 3PY
Telephone +01425621262 or email mark@sds-group.co.uk

Data Protection Regulator

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone +0303 123 1113 or 01625 545 745
or visit: https:.//ico.org.uk/concerns

DATA SUBJECT ACCESS REQUEST POLICY AND PROCEDURE

CONTENTS

1 PURPOSE

1.1 This policy and procedure establishes an effective, accountable and transparent framework for ensuring compliance with the requirements for data subject access request by the *GDPR.*

2 SCOPE

2.1 This policy and procedure applies across all entities or subsidiaries owned, controlled, or operated by SDS Group and to all employees, including part-time, temporary, or contract employees, that handle all personal data.

3 POLICY STATEMENT

3.1 The GDPR details rights of access to both manual data (which is recorded in a relevant filing system) and electronic data for the data subject. This is known as a Data Subject Access Request (DSAR).

3.2 Under the GDPR, organisations are required to respond to subject access requests within one month. Failure to do so is a breach of the GDPR and could lead to a complaint being made to the Data Protection Regulator.

3.3 This policy informs staff of the process for supplying individuals with the right of access to personal data and the right of access to staff information under the General Data Protection Regulation (hereinafter called GDPR). Specifically:

- All staff need to be aware of their responsibilities to provide information when a data subject access request is received. When a subject access request is received, it should immediately be reported to the Data Protection Officer to log and track each request.
- Requests must be made in writing (template form is provided, but not mandatory).
- The statutory response time is one month.
- Requests should include the full name, date of birth and address of the person seeking access to their information. To comply with the GDPR, information relating to the individual must only be disclosed to them or someone with their written consent to receive it.
- No fee can be charged for initial DSAR for all types of records, whether manual or electronic format.

4 PROCEDURE

How should DSARs be processed after receiving

When a subject access request is received from a data subject it should immediately be reported to the Data Protection Officer who will log and track each request. If you are asked to provide information, you will need to consider the following before deciding how to respond:

- Under GDPR Articles 7(3), 12, 13, 15-22 data subjects have the following rights:
  - to be informed;
  - to access their own data;
  - to rectification;
  - to erasure (Right to be Forgotten);
  - to restriction of processing;
  - to be notified;
  - to data portability;
  - to object;
  - to object to automated decision making.

- Requests must be made in writing (template form is attached, but is not mandatory). All DSARs received by email, mail, fax, social media, etc. must be processed.
- The type of access you must provide and the fee you are allowed to charge may vary depending on how the records are held. It does not have to state 'subject access request' or 'data protection' to constitute a request under the GDPR.
- If a request has already been complied with and an identical or similar request is received from the same individual a fee can be charged for the second request unless a reasonable interval has elapsed.
- The statutory response time is one month.
- Requests should include the full name, date of birth and address of the person seeking access to their information. To comply with the GDPR, information relating to the individual must only be disclosed to them or someone with their written consent to receive it.
- Before processing a request, the requestor's identity must be verified. Examples of suitable documentation include:
  - Valid Passport
  - Valid Identity Card
  - Valid Driving Licence
  - Birth Certificate along with some other proof of address e.g. a named utility bill (no longer than 3 months old)

Fees

4.1 No fee can be charged for providing information in response to a data subject access request, unless the request is 'manifestly unfounded or excessive', in particular because it is repetitive.
If SDS Group receives a request that is manifestly unfounded or excessive, it will charge a reasonable fee taking into account the administrative costs of responding to the request. Alternatively, SDS Group will be able to refuse to act on the request.

Subject access requests made by a representative or third party

4.2 Anyone with full mental capacity can authorise a representative/third party to help them make a data subject access request. Before disclosing any information, SDS Group must be satisfied that the third party has the authority to make the request on behalf of the requestor and that the appropriate authorisation to act on their behalf is included (see *Data Request Form*).

Complaints

4.3 If an individual is dissatisfied with the way SDS Group have dealt with their subject access request, they should be advised to invoke the SDS Group complaints process. If they are still dissatisfied, they can complain to the Data Protection Regulator.

5 RESPONSIBILITIES

Compliance, monitoring and review

5.1 The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing subject access rights at SDS group rests with the Data Protection Officer.

5.2 All operating units' staff that deal with personal data are responsible for processing this data in full compliance with the relevant SDS Group policies and procedures.

Records management

5.3 Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised SDS Group recordkeeping system.

5.4 All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

6 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

DSAR: data subject access request

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

7 RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- SDS Group Data Protection Policy (GDPR/DPP/SDS01_01)
- Subject Access Request Form (GDPR/DSARP/SDS02_03)

8 FEEDBACK AND SUGGESTIONS

8.1 SDS Group employees may provide feedback and suggestions about this document by emailing mark@sds-group.co.uk.

9 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Managing Director & Data Protection Officer

Approval and Review	Details
Data Protection Officer	Chave Anderson
Next Review Date	01/05/2021

Approval and Amendment History	Details
Original Approval Authority and Date	Mark Coleman 01/05/2018
Amendment Authority and Date	Draft: Managing Director 24/04/2018
	Review: Managing Director 27/04/2018
	Audit/Approval: Managing Director 01/05/2018
	Final: Managing Director 15/05/2018

SUBJECT ACCESS REQUEST FORM

If you want us to supply you with a copy of any personal data we hold about you, please complete this form and send it the address below. You are currently entitled to receive this information under the EU General Data Protection Regulation (GDPR). We will also provide you with information about any processing of your personal data that is being carried out, the retention periods which apply to your personal data, and any rights to rectification, erasure, or restriction of processing that may exist.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and responding to your request.

Please send your completed form and proof of identity to: SDS Group

Section 1: Details of the person requesting information

Your full name:	
Your address:	
Your telephone number:	
Your email address:	

Section 2: Are you the data subject?

Please tick the appropriate box.

- o **YES**: I am the data subject. I enclose proof of my identity (see below). Please proceed to Section 4.
- o **NO**: I am acting on behalf of the data subject. I have enclosed the data subject's written authority and proof of the data subject's identity and my own identity (see below). Please proceed to Section 3.

To ensure we are releasing data to the right person we require you to provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send the originals) of one of both of the following:

1) **Proof of Identity.** We need one of the following: passport, photo driving license, national identity card, birth certificate.
2) **Proof of Address.** We need one of the following: utility bill, bank statement, credit card statement (no more than 3 months old); current driving license; local authority tax bill.

If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

Section 3: Details of the data subject

Your full name:	
Your address:	
Your telephone number:	
Your email address:	

Section 4: What information are you seeking?

Please describe the information you are seeking. Please provide any relevant details you think will help us to identify the information you require.

……
……
……
……
……
……
……
……
……
……
……
……
……

Please note that if the information you request reveals details directly or indirectly about another person we will have to seek the consent of that person before we can let you see that information. In certain circumstances, where disclosure would adversely affect the rights and freedoms of others, we may not be able to disclose the information to you, in which case you will be informed promptly and given full reasons for that decision.

While in most cases we will be happy to provide you with copies of the information you request, we nevertheless reserve the right, in accordance with Article 12 of the GDPR to charge a fee or refuse the

request if it is considered to be “manifestly unfounded or excessive”. However, we will make every effort to provide you with a satisfactory form of access or summary of information if suitable.

Section 5: Information about the data collection and processing

If you want information about any of the following, please tick the boxes:

- o Why we are processing your personal data
- o To whom your personal data are disclosed
- o The source of your personal data

Section 6: Disclosure of CCTV images

If the information you seek is in the form of video images captured by our CCTV security cameras, would you be satisfied with viewing these images?

- o **YES**
- o **NO**

Section 7: Declaration

Please note that any attempt to mislead may result in legal action.

I confirm that I have read and understood the terms of this Data Subject Access Request Form and certify that the information given in this application to SDS Group is true. I understand that it is necessary for SDS Group to confirm my / the data subject’s identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

…….. ……

Signature Date

Attachments:

I am enclosing the following copies as proof of identity:

……

……

……

……

……

……

……

……

……

DATA BREACH NOTIFICATION POLICY AND PROCEDURE

CONTENTS

1 PURPOSE

This policy and procedure establishes an effective, accountable and transparent framework for ensuring compliance with the requirements for Data Breach Notification by the *GDPR.*

2 SCOPE

This policy and procedure applies across all entities or subsidiaries owned, controlled, or operated by SDS Group and to all employees, including part-time, temporary, or contract employees, that handle Restricted data.

3 POLICY STATEMENT

Any staff member who suspects that a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data might have occurred, must immediately notify the Data Protection Officer and provide a description of the circumstances. Notification of the incident can be made via e-mail, by telephone, or in person.

The Data Protection Officer will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Data Protection Officer will follow the data breach notification procedure based on the criticality and quantity of the personal data involved. For severe personal data breaches, SDS Group's Executive Team will initiate and chair an emergency response team to coordinate and manage the personal data breach response.

4 NOTIFICATION PROCEDURE

4.1 All personal data breaches must be reported immediately to SDS Group’s Data Protection Officer.

4.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Data Protection Regulator is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

4.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Art 4.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

4.4 Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of SDS Group’s Data Protection Officer;
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by SDS Group to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

5 RESPONSIBILITIES

Compliance, monitoring and review

5.1 The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing digitisation activities at SDS Group rests with the Data Protection Officer.

5.2 All operating units’ staff that deal with personal data are responsible for processing this data in full compliance with the relevant SDS Group policies and procedures.

Records management

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised SDS Group recordkeeping system.

All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

6 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

7 RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- SDS Group Data Protection Policy (GDPR/DPP/SDS01_01)

8 FEEDBACK AND SUGGESTIONS

8.1 SDS Group employees may provide feedback and suggestions about this document by emailing mark@sds-group.co.uk.

9 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Managing Director & Data Protection Officer
Data Protection Officer	Chave Anderson
Next Review Date	01/05/2021

Approval and Amendment History	Details
Original Approval Authority and Date	Mark Coleman 01/05/2018
Amendment Authority and Date	Draft: Managing Director 24/04/2018
	Review: Managing Director 14/05/2019
	Audit/Approval: Managing Director 01/05/2018
	Final: Managing Director 15/05/2019

DATA BREACH NOTIFICATION CLIENT PROCEDURE

CONTENTS

1 PURPOSE

This policy and procedure establishes an effective, accountable and transparent framework for ensuring compliance with the requirements for Data Breach Notification by the *GDPR.*

2 SCOPE

This procedure applies for Client and Client Subjects identification of a Breach of Data Protection data.

3 POLICY STATEMENT

Any Client or Client Subject who suspects that a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data might have occurred, must immediately notify the Data Protection Officer and provide a description of the circumstances. Notification of the incident can be made via e-mail, by telephone, or in person.

The Data Protection Officer will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Data Protection Officer will follow the data breach notification procedure based on the criticality and quantity of the personal data involved. For severe personal data breaches, SDS Group's Executive Team will initiate and chair an emergency response team to coordinate and manage the personal data breach response.

4 NOTIFICATION PROCEDURE

4.1 All personal data breaches must be reported immediately to SDS Group’s Data Protection Officer.

4.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Data Protection Regulator is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

4.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Art 4.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

4.4 Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of SDS Group’s Data Protection Officer;
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by SDS Group to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

4.5 Data breach notifications should be sent via the following:-

- Email to the Data Protection Officer gdpr@sds-group.co.uk
- In Person at SDS Group, Data Protection Officer, SDS Group, Suite 5 Hello House, 135 Somerford Road, Christchurch, Dorset, BH23 3PY
- Telephone to 01425 621262

5 RESPONSIBILITIES

Compliance, monitoring and review

5.1 The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing digitisation activities at SDS Group rests with the Data Protection Officer.

5.2 All operating units' staff that deal with personal data are responsible for processing this data in full compliance with the relevant SDS Group policies and procedures.

Records management

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised SDS Group recordkeeping system.

All records relevant to administering this procedure will be maintained for a period of 5 years.

6 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

7 RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- SDS Group Data Protection Policy (GDPR/DPP/SDS01_01)
- Data Breach Notification Policy and Procedure (GDPR/DBNP/SDS03_01)

8 FEEDBACK AND SUGGESTIONS

8.1 Client or Client subjects may provide feedback and suggestions about this document by emailing mark@sds-group.co.uk.

9 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Managing Director & Data Protection Officer
Data Protection Officer	Chave Anderson
Next Review Date	01/05/2021

Approval and Amendment History	Details
Original Approval Authority and Date	Mark Coleman 01/05/2018
Amendment Authority and Date	Draft: Managing Director 24/04/2018
	Review: Managing Director 10/05/2019
	Audit/Approval: Managing Director 15/05/2019
	Final: Managing Director 15/05/2019

DATA PROTECTION IMPACT ASSESSMENT POLICY AND PROCEDURE

CONTENTS

1 PURPOSE

This policy and procedure establishes an effective, accountable and transparent framework for ensuring compliance with the requirements for data protection impact assessment by the GDPR.

2 SCOPE

This policy and procedure applies across all entities or subsidiaries owned, controlled, or operated by SDS Group and to all employees, including part-time, temporary, or contract employees, that handle personal data.

3 POLICY STATEMENT

Data Protection Impact Assessments (DPIA) are used to identify and mitigate against any data protection related risks arising from a new project, service, product, or process, which may affect the organization (Data Controller) or the individuals (Data Subjects).

When is DPIA necessary

3.1 DPIA is necessary:

- Before the implementation of new technologies or processes, or before the modification of existing technologies or processes;
- Data processing is likely to result in a high risk to the rights and freedoms of individuals.

3.2 Processing that is likely to result in a high risk includes (but is not limited to):

- Systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals;
- Large scale processing of special categories of data or personal data relation to criminal convictions or offences;

Should the Regulator be consulted on completion of the DPIA

3.3 If, during the DPIA process, the Data Controller has identified and taken measures to mitigate any risks to personal data, it is not necessary to consult with the Regulator before proceeding with the changes.

3.4 If the DPIA suggests that any identified risks cannot be managed and the residual risk remains high, you must consult with the Regulator before moving forward with the project.

3.5 Regardless of whether or not consultation with the Regulator is required, your obligations of retaining a record of the DPIA and updating the DPIA in due course remain.

3.6 Even if consultation is not required, the DPIA may be reviewed by the Regulator at a later date in the event of an audit or investigation arising from your use of personal data.

4 PROCEDURE

Steps for conducting DPIA

4.1 **Evaluate data flows.** Each department of SDS Group data collection will evaluate how personal information will be collected, stored, used and deleted as part of the new (or modified) system or process. It will Identify what kinds of data will be used as part of the new (or modified) system or process and who will have access to the data.

4.2 **Identify data protection and related risks.** SDS Group will identify all risks to Data Subjects or to the organisation (Data Controller) that are related to personal data protection. For each risk SDS Group will assign a risk category (High/Medium/Low).

4.3 **Assign risk mitigation measures.** For each Risk identified, SDS group will assign a risk mitigation measures. Focus will be given to mitigating measures for risks with High and Medium impact category.

4.4 **Further actions.** SDS Group may at times consider if the Regulator should be consulted for the DPIA. SDS Group will plan regular DPIA reviews and updates where required.

5 RESPONSIBILITIES

Compliance, monitoring and review

5.1 The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing data protection impact assessment activities at SDS Group rests with the Data Protection Officer.

5.2 All operating units' staff that deal with personal data are responsible for processing this data in full compliance with the relevant SDS Group policies and procedures.

Records management

5.3 Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised SDS Group recordkeeping system.

5.4 All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

6 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

7 RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- SDS Group Data Protection Policy (GDPR/DPP/SDS01_01)
- Data Protection Impact Assessment Form (GDPR/DPIA/SDS04_02)

8 FEEDBACK AND SUGGESTIONS

8.1 SDS Group employees may provide feedback and suggestions about this document by emailing mark@sds-group.co.uk.

9 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Managing Director & Data Protection Officer
Data Protection Officer	Chave Anderson
Next Review Date	01/05/2021

Approval and Amendment History	Details
Original Approval Authority and Date	Managing Director 01/05/2018
Amendment Authority and Date	Draft: Managing Director 24/04/2018
	Review: Managing Director 27/04/2018
	Audit/Approval: Managing Director 01/05/2018
	Final: Managing Director 15/05/2018

DATA TRANSFERS POLICY

CONTENTS

1 PURPOSE

This policy and procedure establishes an effective, accountable and transparent framework for ensuring compliance with the requirements for data transfers by the GDPR.

2 SCOPE

This policy and procedure applies across all entities or subsidiaries owned, controlled, or operated by SDS Group and to all employees, including part-time, temporary, or contract employees, that handle personal data and/or personal data transfers.

3 POLICY STATEMENT

3.1 The SDS Group services/entities may transfer personal data to internal or third party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. third countries), they must be made in compliance with an approved transfer mechanism. The SDS Group services/entities may only transfer personal data where one of the transfer scenarios list below applies:

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

Transfers between SDS Group services/entities

3.2 In order for The SDS Group to carry out its operations effectively across its various services/entities, there may be occasions when it is necessary to transfer personal data internally from one Entity to another, or to allow access to the personal data from an overseas location. Should this occur, the SDS Group service/entity sending the personal data remains responsible for ensuring protection for that personal data.

3.3 The SDS Group handles the transfer of personal data between SDS Group services/entities, where the location of the recipient entity is a third country, using the binding corporate rules transfer mechanism. Binding corporate rules provide legally binding, enforceable rights on data subjects with regard to the processing of their personal data and must be enforced by each approved SDS Group service/entity, including their employees. Only transfer the minimum amount of personal data necessary for the particular purpose of the transfer (for example, to fulfil a transaction or carry out a particular service). Ensure adequate security measures are used to protect the personal data during the transfer (including password-protection and encryption, where necessary).

Transfers to Third Parties

3.4 Each SDS Group service/entity will only transfer personal data to, or allow access by, third parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where third party processing takes place, each SDS Group service/entity will first identify if, under applicable law, the third party is considered a data controller or a data processor of the personal data being transferred.

3.5 Where the third party is deemed to be a data controller, the SDS Group service/entity will enter into, in cooperation with the Data Protection Officer, an appropriate agreement with the controller to clarify each party's responsibilities in respect to the personal data transferred. Where the third party is deemed to be a data processor, the SDS Group service/entity will enter into, in cooperation with the Data Protection Officer, an adequate processing agreement with the data processor. The agreement must require the data processor to protect the personal data from further disclosure and to only process personal data in compliance with the SDS Group instructions. In addition, the agreement will require the data processor to implement appropriate technical and organisational measures to protect the personal data as well as procedures for providing notification of personal data breaches.

3.6 The SDS Group has a 'Standard Data Processing Agreement' document that, should be used as a baseline template. When an SDS Group service/entity is outsourcing services to a third party (including cloud computing services), they will identify whether the third party will process personal data on its behalf and whether the outsourcing will entail any third country transfers of personal data. In either case, it will make sure to include, in cooperation with the SDS Group Data Protection Officer, adequate provisions in the outsourcing agreement for such processing and third country transfers.

4 RESPONSIBILITIES

Compliance, monitoring and review

4.1 The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing data transfers activities at SDS Group rests with the Data Protection Officer.

4.2 All operating units' staff that deal with personal data are responsible for processing this data in full compliance with the relevant SDS Group policies and procedures.

Records management

4.3 Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised SDS Group recordkeeping system.

4.4 All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

5 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

6 RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- SDS Group Data Protection Policy (GDPR/DPP/SDS01_01)
- SDS Standard Data Processing Agreement (GDPR/DTP/SDS05_02)

7 FEEDBACK AND SUGGESTIONS

7.1 SDS Group employees may provide feedback and suggestions about this document by emailing mark@sds-group.co.uk.

8 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Managing Director & Data Protection Officer
Data Protection Officer	Chave Anderson
Next Review Date	01/05/2021

Approval and Amendment History	Details
Original Approval Authority and Date	Managing Director 01/05/2018
Amendment Authority and Date	Draft: Managing Director 24/04/2018
	Review: Managing Director 27/04/2018
	Audit/Approval: Managing Director 01/05/2018
	Final: Managing Director 15/05/2018

DATA SECURITY POLICY

CONTENTS

1 PURPOSE

This policy establishes an effective, accountable and transparent framework for ensuring high standards of data security at SDS Group.

2 SCOPE

This policy applies across all entities or subsidiaries owned, controlled, or operated by SDS Group and to all employees, including part-time, temporary, or contract employees.

3 POLICY STATEMENT

Physical security

The SDS Group office is under 24x7 security protection, at both premises level and floor level to ensure only authorized individuals have access to the building and the SDS Group office. At the premises level, the building's perimeter is secured by locked external doors and surround fencing. At the floor level, encrypted Key Fob door control is present to authorize entry to individuals. Employees are granted access to the office only after authorization using the Key Fobs. Critical locations in the office are accessible only to authorized individuals.

Important documents are stored in controlled environments that can only be accessed by pre-authorized individuals. Fire alarms are in place to detect and mitigate damage in the unlikely event of a fire. Regular fire drills are also conducted by the premises management team to educate employees about emergency evacuation procedures. Visitor access to the offices are regulated to ensure that no access is given to secure data. The office is provided with 24x7 power supply, supported by an alternative uninterrupted power supply system to ensure smooth functioning in the event of power failure.

SDS Group hosts its application and data in industry-leading Amazon EU, whose data centre's have been thoroughly tested for security, availability and business continuity.

Application security

All of SDS Group's applications are hosted in Amazon EU. The infrastructure for databases and application servers is managed and maintained by Amazon EU.

At SDS Group, we take a multifaceted approach to application security, to ensure everything from engineering to deployment, including architecture and quality assurance processes complies with our highest standards of security.

Application Architecture

The application is initially protected by Amazon EU's firewall which is equipped to counter regular DDoS attacks and other network related intrusions. The second layer of protection is SDS Group own application firewall which monitors against offending IPs, users and spam. While the application can be accessed only by users with valid credentials, it should be noted that security in cloud-based products is a shared responsibility between the company and the businesses who own those accounts on the cloud. In addition to making it easy for administrators to enforce industry-standard password policies on users, our applications also incorporate features aimed at securing business data on the cloud:

- Configuring secure socket connections to portals;
- Leveraging SAML and custom single sign-on;
- Whitelisting IPs for exclusive access;
- Identity management via Google and Facebook credentials;
- Custom email servers, etc.;

- It should be noted that all account passwords that are stored in the application are one-way hashed and salted.

Access to the application by the SDS Group development team is also controlled, managed and audited. Access to the application and the infrastructure are logged for subsequent audits.

The in-line email attachment URLs for our systems are public by design, to enable us to embed links within the email for end-user ease. This can be made private on customer request.

Application Engineering and Development

Our engineers are trained in industry-leading secure coding standards and guidelines to ensure our products are developed with security considerations from the ground-up. A security review is a mandatory part of application engineering process at SDS Group.

Quality Assurance

Besides functional validation and verification, the quality assurance process at SDS Group also subjects application updates to a thorough security validation. The validation process is performed by a dedicated employees whose goal is to discover and demonstrate vulnerabilities in the application. An update to the application does not get the stamp of approval from the quality assurance team if vulnerabilities (that can compromise either the application or data) are identified.

Data Security

SDS Group takes the protection and security of its customers' data very seriously. SDS Group manages the security of its application and customers' data. However, provisioning and access management of individual accounts is at the discretion of individual business owners.

The SDS Group development team may have access to data on production servers. Changes to the application, infrastructure, web content and deployment processes are documented extensively as part of an internal change control process.

Our products collect limited information about customers - name, email address and phone - which are retained for account creation. Postal address is requested and retained by SDS Group PCI compliant payment processor for billing, along with the date of expiry of credit card and CVV.

SDS Group takes the integrity and protection of customers' data very seriously. We maintain history of two kinds of data: application logs from the system, and application and customers' data. All data is stored in Amazon EU's state of the art cloud computing platform. Backups are taken every day at multiple locations.

Application logs are maintained for a duration of 90 days. Customers' data is backed up in two ways:

1. A continuous backup is maintained in different datacenters to support a system failover if it were to occur in the primary datacenter. Should an unlikely catastrophe occur in one of the datacenters, businesses would lose only five minutes of data.
2. Data is backed up to persistent storage every day and retained for the last seven days.

Different environments are in use for development and testing purposes, access to systems are strictly managed, based on the principles of need to do/know basis appropriate to the information classification, with Segregation of Duties built in, and reviewed on a quarterly basis.

Data Deletion

When an account is deleted, all associated data is archived on secure servers and on request destroyed within 30 business days. SDS Group products also offer data export options which businesses can use if they want a backup of their data before deletion.

Operational Security

SDS Group understands that formal procedures, controls and well-defined responsibilities need to be in place to ensure continued data security and integrity. The company has clear change management processes, logging and monitoring procedures, and fall back mechanisms which have been set up as part of its operational security directives.

Operational security starts right from recruiting an engineer to training and auditing their work products. The recruitment process includes standard background verification checks (including verification of academic records) on all new recruits. All employees are provided with adequate training about the information security policies of the company and are required to sign that they have read and understood the company's security-related policies. Confidential information about the company is available for access only to select authorized SDS Group employees.

Employees are required to report any observed suspicious activities or threats. The human resources team takes appropriate disciplinary action against employees who violate organizational security policies. Security incidents (breaches and potential vulnerabilities) can be reported by customers through our portal at SDS Group.co.uk or via email: mark@sds-group.co.uk.

SDS Group maintains an inventory of all information systems used by employees for development purposes in an internal service desk. Only authorized and licensed software products are installed by employees. No third parties or contractors manage software or information facilities, and no development activity is outsourced. All employee information systems are authorized by the management before they are installed or put to use.

The company has a *Data Protection Policy*, approved by the Directors.

Network Security

Network security is discussed in detail in this section from the perspective of the development center, and the network where the application is hosted.

The SDS Group office network where updates are developed, deployed, monitored and managed is secured by industry-grade firewalls and antivirus software, to protect internal information systems from intrusion and to provide active alerts in the event of a threat or an incident. Firewall logs are stored and reviewed periodically. Access to the production environment is via SSH and remote access is possible only via the office network. Audit logs are generated for each remote user session and reviewed. Also, the access to production systems are always through a multi-factor authentication mechanism.

All SDS Group products are hosted in Amazon EU, with security managed by Amazon EU. Our team monitors the infrastructure 24x7 for stability, intrusions and spam. Every three months, end-to-end vulnerability assessments and penetration tests are performed.

4 RESPONSIBILITIES

Regulatory Compliance

All formal processes and security standards at SDS Group are designed to meet regulations at the industry, state and European Union levels.

Use of our service by customers in the European Economic Area ("EEA"), will include the processing of information relating to their customers. In providing our service, we do not own, control or direct the use of the information stored or processed on our platform at the direction of our customers, and in fact we are largely unaware of what information is being stored on our platform and only access such information as reasonably necessary to provide the service (including to respond to support requests), as otherwise authorized by our customers or as required by law. We are Data Processors for our end customers, but Data Controllers for the customers from whom we collect data on our platform for purposes of the European Union ("EU") on our platform for purposes of the European Union ("EU") General Data Protection Regulation (GDPR). Our EEA based customers, who control their customer data and send it to SDS Group for processing, are the "Controllers" of that data and are responsible for compliance with the GDPR. In particular, SDS Group customers are responsible for complying with the GDPR and relevant data protection legislation in the relevant EEA member state before sending personal information to SDS Group for processing.

As the processors of personal information on behalf of our customers, we follow their instructions with respect to the information they control to the extent consistent with the functionality of our service. In doing so, we implement industry standard security, technical, physical and administrative measures against unauthorized processing of such information and against loss, destruction of, or damage to, personal information as more fully described in SDS Group's Data Protection Policy.

We work with our customers to help them provide notice to their customers concerning the purpose for which personal information is collected and sign Standard Data Processor Agreement (for data processors) with them to legitimize transfers of personal data from EU to processors established in third countries as may be required under the GDPR.

Reporting issues and threats

If you have found any issues or flaws impacting the data security or privacy of SDS Group users, please write to mark@sds-group.co.uk with the relevant information so we can get working on it right away.

Your request will be looked into immediately. We might ask for your guidance in identifying or replicating the issue and understanding any means to resolving the threat right away. Please be clear and specific about any information you give us. We deeply appreciate your help in detecting and fixing flaws in SDS Group, and will acknowledge your contribution to the world once the threat is resolved.

Records management

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised SDS Group recordkeeping system.

All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

Google Analytics

SDS Group on behalf of our clients, offer the option to add Google Analytics to their online systems, this function tracks and reports website traffic. SDS Group have no access to Clients Google Analytics function, and as such harvest any information from the function.

5 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

6 RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- SDS Group Data Protection Policy (GDPR/DPP/SDS01_01)

7 FEEDBACK AND SUGGESTIONS

7.1 SDS Group employees may provide feedback and suggestions about this document by emailing mark@sds-group.co.uk.

8 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Managing Director & Data Protection Officer
Data Protection Officer	Chave Anderson
Next Review Date	01/05/2021

Approval and Amendment History	Details
Original Approval Authority and Date	Managing Director 01/05/2018
Amendment Authority and Date	Draft: Managing Director 24/04/2018
	Review: Managing Director 27/04/2018
	Audit/Approval: Managing Director 01/05/2018
	Final: Managing Director 15/05/2018

REGISTERS

CONTENTS

1 PURPOSE

The purpose of this policy is to specify SDS Group's GDPR registers and mapping.

2 SCOPE

The scope of this policy covers all SDS Group personal data and Client data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location.

3 POLICY STATEMENT

The need to retain personal data varies widely with the type of data. Some personal data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. These registers and mapping help ensure that all applicable regulations and SDS Group's rules on personal data are consistently applied throughout the organisation.

4 RESPONSIBILITIES

4.1 The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing digitisation and web development activities at SDS Group rests with the Data Protection Officer.

4.2 All operating units' staff that deals with personal data is responsible for processing this data in full compliance with the relevant SDS Group policies and procedures.

4.3 Any authorised personnel may complete the registers and mapping.

Records management

4.4 All registers and mappings must be stored and managed in a manner to be able to:

- Locate any existing register or mapping document quickly.
- Enable authorised personnel access to all types of registers or mapping templates.

4.5 All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

5 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Data Backup: data copied to a second location, solely for the purpose of safe keeping of that data

Data Encryption: the process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored

Data Encryption Key: an alphanumeric series of characters that enables data to be encrypted and decrypted

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

6 RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- SDS Group Data Protection Policy (GDPR/DPP/SDS01_01)
- Data Maps (GDPR/REG/SDS07_02)
- Internal data breach register (GDPR/REG/SDS07_03)
- Register of personal data (GDPR/REG/SDS07_04)
- Register of processing activities (GDPR/REG/SDS07_05)

7 FEEDBACK AND SUGGESTIONS

7.1 SDS Group employees may provide feedback and suggestions about this document by emailing mark@sds-group.co.uk.

8 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Managing Director & Data Protection Officer
Data Protection Officer	Chave Anderson
Next Review Date	01/05/2021

Approval and Amendment History	Details
Original Approval Authority and Date	Managing Director 01/05/2018
Amendment Authority and Date	Draft: Managing Director 24/04/2018
	Review: Managing Director 27/05/2018
	Audit/Approval: Managing Director 01/05/2019
	Final: Managing Director 15/05/2019

Data Processor Checklist

Please complete and return to email address mark@sds-group.co.uk

Name of supplier:

Main supplier contact details for all data privacy matters:

REQUIREMENT	YES/NO	COMMENT
Please confirm what sufficient guarantees you can give SDS Group that demonstrates your understanding and implementation of your obligation, as a processor, under the new GDPR legislation, including any certifications or externally audited processes.		
Do your standard contract terms include the new GDPR mandatory provisions?		
Do your standard contract terms propagate down, within a formal contract, to your sub contract providers involved in the service to SDS Group?		
Are you maintaining Data Processing Records? (as outlined in Article 30 of GDPR)		
Please detail all sub-contractors, included in the provision of your service to SDS Group.		
Do you have a documented Breach Notification Process to ensure notification to SDS Group within 72hrs?		
Do you and your sub processors, providing the service to SDS Group, have a documented process for the deletion of subject's records, upon request, from both live or archived records and backups of your systems?		
Can you confirm our right to have personal data deleted or upon termination of contract at no extra cost?		
Does yours and your sub processor/s, involved in the delivery of services to SDS Group, website/software have a data privacy policy and fair processing notice which meet GDPR requirements?		
Do your contracts of employment contain confidentiality and gross misconduct clauses, in the context of customers data privacy?		

Data Protection Officer (DPO)
JOB DESCRIPTION

Job title	Data Protection Officer (DPO)
Department	Data Protection
Reporting to	Managing Director
Job summary	SDS Group DPO is tasked with monitoring compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits. We will take account of our DPO's advice and the information they provide on our data protection obligations. When carrying out a DPIA, we seek the advice of our DPO who also monitors the process. Our DPO acts as a contact point for the ICO. They co-operate with the ICO, including during prior consultations under Article 36, and will consult on any other matter. When performing their tasks, our DPO has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.
Main tasks	Effectively manage and administer and act as the budget holder for the Data Protection Governance financial budget. To monitor compliance with the data protection provisions, with other countries' data protection provisions and with the policies of SDS Group in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits playing a critical role in decisions made relating to data protection. To take the lead in providing expert data protection advice to Managing Director, SDS Group managers and external clients relating to all aspects of data protection. Develop and implement a comprehensive data protection plan and provide advice in this area. To draft agreements relating to the processing of personal information for use with external organisations in order to ensure data protection compliance, this will include but not limited to data disclosure agreements, data processing agreements, data transfer agreements, memorandum of understandings and confidentiality agreements. To provide advice where requested regarding data protection impact assessment process and monitor its performance. To cooperate with the supervisory authority in all matters relating to information governance; and to investigate regulatory complaints in accordance with relevant regulatory requirements. To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation, and to consult, where

	appropriate, with regard to any other matter relating to information governance. To promote data protection compliance and best practice by setting and maintaining standards and procedures, ensuring SDS Group's data protection policies are up to date and disseminate any changes in the legislation to key members of staff. Oversee the management of data subject requests and data protection requests pursuant to individual rights under data protection and privacy legislation. To carry out reviews of SDS Group's decisions to refuse requests under the General Data Protection Regulations where required, whilst ensuring that the original decision made by the Information Management Officer was accurate and, where appropriate, overturn any decisions previously made. Advise on all elements of processing personal data internationally and on the requirements and implications of data protection laws. To provide advice to SDS Group and where appropriate draft privacy notices, fair processing notices, collection statements and any other data protection notices in order to ensure that individuals are aware of our intentions to process their data and ensuring that SDS Group is processing personal data in a fair and lawful manner in line with the individual rights. To investigate and report on any processing, blocking, erasure, destruction and the right to be forgotten notices issued by individuals in accordance with the relevant articles contained within the GDPR, ensuring that the purposes of the processing are compatible with the conditions for processing in accordance with the Regulations and responding to the individual accordingly. Assist in responding to any legal claims issued against the SDS Group for damages relating to breaches of data protection. Liaising where appropriate with the Management Department. To provide advice in relation to any data protection queries regarding the use of social media and report any serious issues to the Managing Director. Undertake and manage data protection audits and reviews across all SDS Group departments that are processing personal data in order to ensure that SDS Group is compliant with the legislation. To manage, investigate and resolve all complaints from individuals in relation to their rights under the GDPR. Ensuring that adequate reporting mechanisms are in place for recording such complaints. Investigate breaches and incidents of data protection, establishing any potential weaknesses in SDS Group's policies and inform the Information Governance and Security Group accordingly. Formally report all compliance issues relating to information governance, including any complaints and breaches of the legislative framework to the Managing Director. Provide advice and assist with all data protection queries relating to projects, programmes and data sharing initiatives. In relation to the performance of these tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

SDS Group GDPR Management Structure

The SDS Group GDPR Management process begins with the Company Managing Director who oversees the whole Data Protection process.

Overall operation of the Data Protection Management and systems is under the authority of the Data Protection Officer who answers directly to the Managing Director.

Day to day operation of the Data Protection Management and operation is under the authority of the SDS Management Team who answers to the Data Protection Officer.

All SDS Staff have a responsibility of maintaining Data Protection at all times.

Clients are encouraged to report any breaches of the Data Protection Act directly to the Managing Director who will initiate a full review of the breaches.

Requests for Subject Data Access can be made by all persons, or their approved representatives, directly to the Data Protection Manager who will supply the relevant information.

DATA RETENTION POLICY

CONTENTS

1 PURPOSE

The purpose of this policy is to specify SDS Group's guidelines for retaining different types of personal data.

2 SCOPE

The scope of this policy covers all SDS Group personal data and Client data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location. These records may be created, received or maintained in hard copy or electronically.

3 POLICY STATEMENT

3.1 The need to retain personal data varies widely with the type of data. Some personal data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. This Data Retention Policy provides guidelines to ensure that all applicable regulations and SDS Group's rules on personal data retention are consistently applied throughout the organisation.

Reasons for data retention

3.2 Some personal data must be retained in order to protect the company's interests, comply with regulatory requirements, preserve evidence, and generally conform to good business practices. Personal data may be retained for one or several of the following reasons:

- Business requirements
- Regulatory requirements
- Possible litigation
- Accident investigation
- Security incident investigation
- Intellectual property preservation

Retention periods

3.3 Different types of data will be retained for different periods of time:

- Personal customer data: Personal data will be held for as long as the individual is a customer of the company plus 3 years.
- Personal employee data: General employee data will be held for the duration of employment and then for 3 years after the last day of contractual employment. Employee contracts will be held for 3 years after last day of contractual employment.
- Personal tax payments will be held for 3 years.
- Records of leave will be held for 3 years.
- Recruitment details: Interview notes of unsuccessful applicants will be held for 3 years after interview. This personal data will then be destroyed.
- Health and Safety: 3 years for records of major accidents and dangerous occurrences.
- Operational data: Most company data will fall in this category. Operational data will be retained for 3 years.
- Critical data including Tax and VAT: Critical data must be retained for 3 years.

For more details, please refer to *Appendix 1 – Data Retention Schedule*

Retention of encrypted data

3.4 If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

Data duplication

3.5 When identifying and classifying SDS Group's personal data, it is important to also understand where that data may be stored, particularly for duplicate copies, so that this policy may be applied to all duplicates of the information.

Data destruction

3.6 When the retention timeframe expires, SDS Group will actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by a member or members of SDS Group's senior management team.
The company specifically directs users not to destroy data in violation of this policy. Destroying data that a user may feel is harmful to himself or herself or destroying data in an attempt to cover up a violation of law or company policy is particularly forbidden.

4 RESPONSIBILITIES

Compliance, monitoring and review

4.1 The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing digitisation and web development activities at SDS Group rests with the Data Protection Officer.

4.2 All operating units' staff that deal with personal data are responsible for processing this data in full compliance with the relevant SDS Group policies and procedures.

Reporting in case of a data breach

4.3 In the case of possible data breach, the staff member(s) who first identifies the breach or incident, must immediately report all details of the incident to the Data Protection Officer.

4.4 The Data Protection Officer is required to report a personal data breach to the competent Data Protection Authority not later than 72 hours after becoming aware of it. The notification must include at least:

- a description of the nature of the breach, including, where possible, the categories and approximate number of data subjects and personal data records concerned;
- the name and contact details of the relevant Data Protection Officer or contact point;
- the likely consequences of the data breach; and
- measures taken or proposed by the controller to address the breach and/or mitigate its effects.

4.5 Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the Data Protection Officer must communicate the breach to the data subject(s) without undue delay. The communication must describe in clear and plain language, the nature of the breach and at least:

- the name and contact details of the relevant Data Protection Officer or contact point;
- the likely consequences of the data breach; and
- measures taken or proposed by the controller to address the breach and/or mitigate its effects.

Records management

4.6 Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised SDS Group recordkeeping system.

4.7 All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

5 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Data Backup: data copied to a second location, solely for the purpose of safe keeping of that data

Data Encryption: the process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored

Data Encryption Key: an alphanumeric series of characters that enables data to be encrypted and decrypted

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

6 RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- SDS Group Data Protection Policy (GDPR/DPP/SDS01_01)
- Data Retention Schedule (GDPR/DRP/SDS10_02)

7 FEEDBACK AND SUGGESTIONS

7.1 SDS Group employees may provide feedback and suggestions about this document by emailing mark@sds-group.co.uk.

8 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Managing Director & Data Protection Officer
Data Protection Officer	Chave Anderson
Next Review Date	01/05/2021

Approval and Amendment History	Details
Original Approval Authority and Date	Managing Director 01/05/2018
Amendment Authority and Date	Draft: Managing Director 24/04/2018
	Review: Managing Director 27/05/2019
	Audit/Approval: Managing Director 01/05/2019
	Final: Managing Director 15/06/2019

ARCHIVING IN THE PUBLIC INTEREST

CONTENTS

1 PURPOSE

1.1 This policy and procedure establishes an effective, accountable and transparent framework for ensuring compliance with the requirements for archiving in the public interest by the *GDPR.*

2 SCOPE

2.1 This policy and procedure applies across all entities or subsidiaries owned, controlled, or operated by SDS Group and to all employees, including part-time, temporary, or contract employees, that handle all personal data.

3 POLICY STATEMENT

3.1 The GDPR provisions do not apply to any personal data which has been processed for Heritage Archiving purposes which may be in the Public Interest, whereby that the application of the GDPR requirements would prevent or impair the achievement of those purposes.

3.2 SDS Group do not extract, copy, store or supply any of the data located in Heritage Archiving to any Third Party Client or Organisation unless with the express permission of the Client originator.

3.3 Items listed below are identified as being part of the Heritage Archiving process.

- Magazine/Journals and Booklets which are in the public domain.
- Photographs/Slides/Negatives and static images whereby names are collected to aid the search function.
- Video/Film/Audio media files of Heritage materials.
- Miscellaneous Ephemeral documents which provide Historical heritage archives.

4 PROVISION TO REMAIN ANONYMOUS

Each person who may be affected by the Archiving in the Public Interest GDPR exemption, continue to have the right to be removed from the archive and remain anonymous.

When a request is received from a data subject it should immediately be reported to the Data Protection Officer who will log and track each request.

The method of removing such data from the Archive will be achieved in one or more of the following ways:

- Under Redaction of data from within the electronic copy.
- Removal of extracted search data.
- Deletion of database entry and removal of electronic copy.

As SDS Group do not own either the Clients Online systems or data, the following process should be followed:

- Requests should be made in the initial instance directly to the Owner of the Online System and data (SDS Group Client).
- The SDS Group Client will then request that the information be removed.
- If any individual requests are made directly to SDS Group, SDS Group will first obtain consent from the Client before any Redaction, Removal or deletion is performed.
- The response time for any consented removal is one month.
- Requests should include the full details of the data to be Redacted, Removed or deleted.

Fees

4.1 No fee will be charged for removing information in response to a data removal request, unless the request is ‘manifestly unfounded or excessive’, in particular because it is repetitive.

If SDS Group receives a request that is manifestly unfounded or excessive, it will charge a reasonable fee taking into account the administrative costs of responding to the request. Alternatively, SDS Group will be able to refuse to act on the request.

Subject access requests made by a representative or third party

4.2 Anyone with full mental capacity can authorise a representative/third party to help them make a data removal request.

Complaints

4.3 If an individual is dissatisfied with the way SDS Group have dealt with their subject access request, they should be advised to invoke the SDS Group complaints process. If they are still dissatisfied, they can complain to the Data Protection Regulator.

5 RESPONSIBILITIES

5.1 The overall responsibility for ensuring compliance with the requests to remove data from Public Interest Archiving within SDS group rests with the Data Protection Officer.

5.2 The recording of the removal of data from Public Interest Archiving is not required.

6 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

DSAR: data subject access request

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

7 RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- SDS Group Data Protection Policy (GDPR/DPP/SDS01_01)

8 FEEDBACK AND SUGGESTIONS

8.1 SDS Group employees may provide feedback and suggestions about this document by emailing mark@sds-group.co.uk.

9 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Managing Director & Data Protection Officer
Data Protection Officer	Chave Anderson
Next Review Date	01/05/2021

Approval and Amendment History	Details
Original Approval Authority and Date	Mark Coleman 01/05/2018
Amendment Authority and Date	Draft: Managing Director 24/04/2018
	Review: Managing Director 27/04/2019
	Audit/Approval: Managing Director 01/05/2019
	Final: Managing Director 15/05/2019

SDS GROUP AS A DATA PROCESSOR ACTIVITIES

CONTENTS

1 PURPOSE

This policy and procedure establishes the method in which SDS Group undertake the role of Data Processor for ensuring compliance with the requirements for data transfers by the GDPR.

2 SCOPE

This policy and procedure applies across all entities or subsidiaries owned, controlled, or operated by SDS Group and to all employees, including part-time, temporary, or contract employees, that handle personal data and/or personal data transfers.

3 POLICY STATEMENT

3.1 The SDS Group services offered may require the collection / storage / retention of personal information data to ensure that the Clients service requirements are fully met.

3.2 The following processes may be employed to enable SDS Group to meet these requirements:

- Collection of Client based hard copy archives or documentation.
- The transfer via approved secure methods, electronic data from Clients.
- Pre-preparation including checking suitability of scanning and location of personal data which may be identified to meet the Clients requirements.
- Preparation activities which may involve collection of personal data in line with Clients requirements.
- Scanning activities which may involve collection of personal data in line with Clients requirements.
- General electronic activities which may be required to improve / clean up / prepare files for conversion to final data format.
- Optical Character Recognition to enable Client search function requirements to be obtained.
- Final formatting to the Clients preferred electronic data format. Jpg / tif / pdf etc.
- Secure database data import / input to enable records / items to be found easily or located in a defined manner as per the Clients instructions.
- Transfer of digital copy to secure servers for online cloud storage or via suitable secure alternative to the Client themselves. Encrypted USB / HDD's etc.
- Backup and retention to ensure recovery of systems or digital data as per agreement with Clients.

3.3 In order for The SDS Group to carry out its operations effectively to meet the Client requirements, the following personal data may be collected:

- Name
- Address
- Date of Birth
- Date Died
- Date Started and / or Date Left
- House
- Personal Military information such as Rank, Detachment, Honours, Grave Reference and Others
- Client Company Information

3.4 The SDS Group only uses authorised and trained employees to perform any task required to meet the Clients requirements all of which are required to complete a Non-disclosure agreement.

3.5 All Clients supplied hard copy or digital archives will be stored in a secure environment.

3.6 SDS retains no rights of ownership of any data which we scan or process for our clients. All copyrights and proprietorships remain with our clients. Our clients can have all their data returned to them at request without any penalty or forfeit.

3.7 The SDS Group do not own any Client site or system and as such each Client may use SDS Group to host their system or may host it themselves. Systems hosted on Clients own servers etc. are deemed to be outside of SDS Group GDPR requirements.

3.8 All personal data collected by SDS Group on behalf of Clients requirements is collected in agreement with the Clients own GDPR commitments.

3.9 SDS Group will only collect personal data in line with the Clients agreed requirements.

3.10 All Clients systems are provided with encrypted password and username protection, the Client may request for this function to be removed but any personal data affected will remain the responsibility of the Client.

3.11 Individual persons may request any information to be removed for SDS Group hosted Client systems at any time without incurring any fees; however SDS Group will seek permission from the Client prior to performing this action.

3.12 Clients may request any information to be removed / hidden at any time without incurring any fees.

3.13 All Cloud services hosted by SDS Group are regularly SOAK & Stress tested and hosted on UK based servers by Amazon EU.

3.14 Disposal of Clients hard copy or electronic archives are undertaken in agreement to the Clients requirements, shredding facilities are available and are performed by approved Third Party companies onsite with a SDS Group approved representative in attendance at all times, on completion a certificate will be provided.

4 RESPONSIBILITIES

4.1 The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing data transfers activities at SDS Group rests with the Data Protection Officer.

4.2 All operating units' staff that deals with personal data is responsible for processing this data in full compliance with the relevant SDS Group policies and procedures.

5 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

6 RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- SDS Group Data Protection Policy (GDPR/DPP/SDS01_01)
- SDS Standard Data Processing Agreement (GDPR/DTP/SDS05_02)

7 FEEDBACK AND SUGGESTIONS

7.1 SDS Group employees may provide feedback and suggestions about this document by emailing mark@sds-group.co.uk.

8 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Managing Director & Data Protection Officer
Data Protection Officer	Chave Anderson
Next Review Date	01/05/2021

Approval and Amendment History	Details
Original Approval Authority and Date	Managing Director 01/05/2018
Amendment Authority and Date	Draft: Managing Director 24/04/2018
	Review: Managing Director 27/04/2019
	Audit/Approval: Managing Director 01/05/2019
	Final: Managing Director 15/05/2019

Data Protection Impact Assessment (DPIA) Form

Section 1				Section 2		
Data Processing Activity	Personal Data Involved (Data Categories)	Purposes for Processing	Necessity and Proportionality of the Processing	Risks to Data Subjects	Risk Category	Risk Mitigation Measures
Order Reciept	Only Client Information	Acceptance of Order	Required and Minor			
Preperation Process	Name	Database Entry & Search Function	Required inline with Client Information Requirement			
Preperation Process	Address	Database Entry & Search Function	Required inline with Client Information Requirement where required			
Preperation Process	Date of Birth	Database Entry & Search Function	Required inline with Client Information Requirement where required			
Preperation Process	Date Started	Database Entry	Required inline with Client Information Requirement where required			
Preperation Process	Date Left	Database Entry	Required inline with Client Information Requirement where required			
Scanning Process	Name	Creation of Digitised Filename	Required and Minor			
Clean Up Process	All as above	Tidy up of digitised Files	Required and Minor			
Optical Character Recognition	All as above	Bodytext Search Function Capture	Required and Minor			
Pdf Creation	Name	Digitised Filename	Required and Minor			
Data Extraction	Name	Database Entry & Search Function	Required and Important to meet Clients System requirements			
Data Extraction	Address	Database Entry & Search Function	Required and Important to meet Clients System requirements			
Data Extraction	Date of Birth	Database Entry & Search Function	Required and Important to meet Clients System requirements			
Data Extraction	Date Started	Database Entry	Required and Important to meet Clients System requirements			
Data Extraction	Date Left	Database Entry	Required and Important to meet Clients System requirements			
Online Digital Storage	All as above	Client Requested Display & Search Functionality	Required and Important to meet Clients System requirements			

Data Retention Schedule

Controller of Data Processing:		Last modified (date):	
Type of entity:		Last modified by (name):	
Country of Registration:			
National Identity Number:			
Address:			
Phone Number:			
E-mail Address:			
Website:			
Name of Data Protection Officer (DPO):			
Address:			
Phone number:			
Mobile phone:			
E-mail:			

Data Retention Schedule						
Data Section	Type of Record	Retention Period			Justification	Statutory Provisions (if applicable)
		Number	Period	Counted from		
Personal customer data						
Personal employee data						
Personal tax payments						
Records of leave						
Recruitment details						
Health and safety						
Operational data						
Critical data						