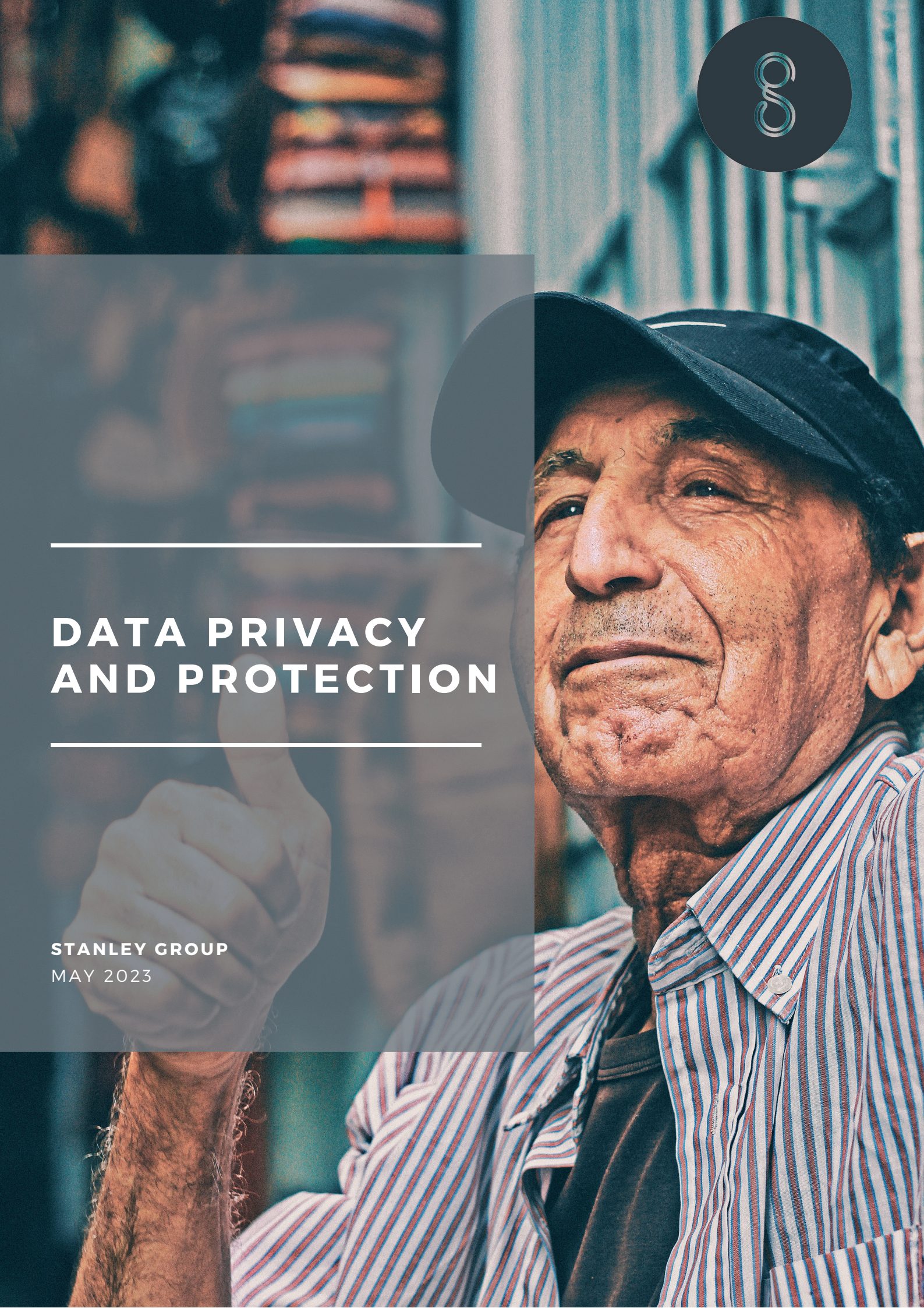

DATA PRIVACY AND PROTECTION

STANLEY GROUP

MAY 2023

Stanley Group Consultants

Data Privacy Statement

Your Privacy

We take your privacy very seriously and *we* ask that you read this privacy notice carefully as it contains important information on who *we* are, how and why *we* collect, store, use and share personal data, your rights in relation to your personal data and on how to contact *us* and supervisory authorities in the event you have a question, concern or complaint.

Italicised words in this privacy notice have the meaning set out in the Glossary of Terms at the end of this document.

Who we are

Stanley Group uses and is responsible for the way in which we process, record and manage certain personal data about you. When *we* do so *we* are required to comply with *data protection regulation,* and *we* are responsible as a *data controller* of that personal data for the purposes of those laws.

We are a company whose office is at 483 Green Lanes, Palmers Green, London N13 4BS, United Kingdom of Great Britain and Northern Ireland.

The personal data we collect and use

In providing our service to you *we* may collect the following personal data when you provide it to *us*:

- *Your contact information,* including name, address, telephone and email address information
- *Your identity information*, including date of birth, passport and driving licence details, National Insurance number, address verification (e.g. utility bills) and any other identify information we are required to collect within jurisdiction in which you reside or in which we operate or provide services on your behalf
- *Financial information,* including your income and expenditure, property, investments and information about other assets, and any mortgage loans and other secured and unsecured loans and credit cards
- *Your employment status*
- *Information about your lifestyle, for example nicotine and/or alcohol consumption*
- *Health information*
- *Details of any vulnerability*
- *Details of your dependents and/or beneficiaries under a policy* ***(If you are providing information about another person, we expect you to ensure that they know you are doing so and are content with their information being provided to us. You might find it helpful to show them this privacy notice and if they have any concerns please contact us in one of the ways described below.)***
- *Information about any existing business interests and/or potential conflicts of interest*
- *Criminal and background checks, where we are required to obtain and record this information, for example in matters of employment*

Information collected from other sources

We also obtain personal data from other sources in providing our *intermediary services*. Where *we* obtain this information from another party it is their responsibility to make sure they explain that they will be sharing personal data with *us* and, where necessary, ask permission before sharing information with *us*.

The personal data *we* obtain from other sources may include the following:

- From identification and verification checking agencies:
  - *identity information*
  - *sanction check information*
- Solicitors and accountants:
  - Details of wills and/or Trusts
  - Business accounts

Personal data (shown in table)

- How *we* use your personal data
- The lawful bases upon which *we* collect and use your personal data
- With whom *we* routinely share your personal data

Rationale/Reason for Processing	Lawful Basis for Processing	Third party recipients linked to that activity
To provide you with intermediary services	Performance of a contract Consent for special categories of data	Our clients, product providers and consultants

To submit tenders for services or participation in arrangement of contractual obligations	Performance of a contract Consent for special categories of data	Our clients, product providers and consultants
To retain records of any services or advice provided to you by us in order to defend legal claims or complaints	Legitimate interests	External suppliers of data storage and data hosting services to retain records on our behalf.
To provide you with details of products and services from us and third parties that may be of interest to you in accordance with your preferences.	Consent	

Special category data

Certain types of personal data are considered more sensitive and so are subject to additional levels of protection under data protection legislation. These are known as 'special categories of data' and include data concerning your health, racial or ethnic origin, genetic data and sexual orientation. Data relating to criminal convictions or offences is also subject to additional levels of protection. *We* may process:

- *health information* and *lifestyle information* when providing *intermediary services* in relation to a protection insurance product for the purposes of services supply to our clients or Group projects/programmes of work

In addition to the lawful basis for processing this information set out in the above table, *we* will be processing it either (i) for advising on, arranging or administering an insurance contract or (ii) for the establishment, exercise or defence of legal claims.

Whether information must be provided by you, and if so why

We will tell you if providing some personal data is optional, including if *we* ask for your consent to process it. In all other cases you must provide your personal data for *us* to provide you with *intermediary services*.

How long your personal data will be kept

We only retain your data for so long as it is necessary to fulfil the purpose for which it was collected. There are regulatory and legislative requirements which oblige us to keep certain data for longer, and to comply with those regulatory requirements we keep that data for seven years. In very limited circumstances, we may be required to keep some specific information for longer, but we regularly review our retention obligations to ensure we don't keep personal information longer than we are legally obliged to.

If you want details of the statutory retention periods for various product types, please contact us and we will obtain the latest legal position on your behalf.

Transfer of your information out of the EEA

We will not transfer your personal data outside of the European Economic Area. However, product providers, lenders and investment managers may administer your data and/or policy, as well as any existing contract(s) for services you may have with them for the provision of other services, from centres in countries outside Europe (such as India and the USA). Such countries do not have the same data protection laws as the United Kingdom or the EEA. However, they are required to put into place a European Commission-approved contract that that will safeguard your privacy rights and give you remedies in the unlikely event of a security breach.

Your rights

You have legal rights under *data protection regulation* in relation to your personal data. These are set out under the below headings:

- To access personal data
- To restrict how *we* use personal data
- To object to how *we* use personal data
- To ask *us* to transfer personal data to another organisation
- To find out more about how *we* use personal data

We will ask you for proof of identity when making a request to exercise any of these rights. *We* do this to ensure *we* only disclose information or change your details where *we* know *we* are dealing with the right individual.

We will not ask for a fee, unless *we* think your request is unfounded, repetitive or excessive, or the data request is complex, or you ask for multiple copies of the same information. Where a fee is necessary, *we* will inform you before proceeding with your request. We withhold the right to decline your request where we are authorised by regulation and/or legislation to do so.

We aim to respond to all valid requests within one month. It may however take us longer if the request is particularly complicated or you have made several requests. *We* will always let you know if *we* think a response will take longer than one month. To speed up *our* response, *we* may ask you to provide more detail about what you want to receive or are concerned about.

We may not always be able to fully address your request, for example if it would impact the duty of confidentiality *we* owe to others, or if *we* are otherwise legally entitled to deal with the request in a different way.

To access personal data

You can ask *us* to confirm whether or not *we* have and are using your personal data. You can also ask to get a copy of your personal data from *us* and for information on how *we* process it.

To rectify / erase personal data

You can ask that *we* rectify any information about you which is incorrect. *We* will be happy to rectify such information but

would need to verify the accuracy of the information first.

You can ask that *we* erase your personal data if you think *we* no longer need to use it for the purpose *we* collected it from you.

You can also ask that *we* erase your personal data if you have either withdrawn your consent to *us* using your information (if *we* originally asked for your consent to use your information) or exercised your right to object to further legitimate use of your information, or where *we* have used it unlawfully or where *we* are subject to a legal obligation to erase your personal data.

We may not always be able to comply with your request, for example where *we* need to keep using your personal data to comply with *our* legal obligation or where *we* need to use your personal data to establish, exercise or defend legal claims.

To restrict our use of personal data

You can ask that *we* restrict *our* use of your personal data in certain circumstances, for example

- where you think the information is inaccurate and *we* need to verify it;
- where *our* use of your personal data is not lawful, but you do not want *us* to erase it;
- where the information is no longer required for the purposes for which it was collected but *we* need it to establish, exercise or defend legal claims; or
- where you have objected to *our* use of your personal data, but *we* still need to verify if *we* have overriding grounds to use it.

We can continue to use your personal data following a request for restriction where *we* have your consent to use it; or *we* need to use it to establish, exercise or defend legal claims, or *we* need to use it to protect the rights of another individual or a company.

To object to use of personal data

You can object to any use of your personal data which *we* have justified based on our legitimate interest if you believe your fundamental rights and freedoms to data protection outweigh *our* legitimate interest in using the information. If you raise an objection, *we* may continue to use the personal data if *we* can demonstrate that *we* have compelling legitimate interests to use the information.

To request a transfer of personal data

You can ask *us* to provide your personal data to you in a structured, commonly used, machine-readable format, or you can ask to have it transferred directly to another *data controller* (e.g. another company).

You may only exercise this right where *we* use your personal data to perform a contract with you, or where *we* asked for your consent to use your personal data. This right does not apply to any personal data which *we* hold or process outside automated means.

You can contact us for more information

If you are not satisfied with the level of information provided in this privacy notice, you can ask *us* about what personal data *we* have about you, what *we* use your information for, who *we* disclose your information to, whether *we* transfer it abroad, how *we* protect it, how long *we* keep it for, what rights you have, how you can make a complaint and from where *we* obtained your data.

If you would like to exercise any of the above rights, please:

- email or write to our Data Protection Officer at info@stanleygroup.org or 483 Green Lanes, Palmers Green, London, N13 4BS;
- let us have enough information to identify you, e.g. name, address, date of birth;
- let us have proof of your identity and address (a copy of your driving licence or passport and a recent utility or credit card bill); and
- let us know the information to which your request relates.

Keeping your personal data secure

We have appropriate security measures in place to prevent personal data from being accidentally lost or used or accessed in an unauthorised way. *We* limit access to your personal data to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. *We* will notify you and any applicable regulator of a suspected data security breach where *we* are legally required to do so.

Our supervisory authority

If you are not happy with the way *we* are handling your information, you have a right to lodge a complaint with the Information Commissioners Office (ICO). It has enforcement powers and can investigate compliance with *data protection regulation* (www.ico.org.uk). We ask that you please attempt to resolve any issues with us before the ICO.

How to contact us

- Please contact our Data Protection Officer if you have any questions about this privacy notice, or the information we hold about you. If you wish to contact our Data Protection Officer, please send an email to info@stanleygroup.org or 483 Green Lanes, Palmers Green, London, N13 4BS;

Declaration

I/We consent for Stanley Group to hold and process My/Our personal data for the purposes of provision of Professional Services, and I/We authorise the transfer of personal information, on a confidential basis and in accordance with the Data Protection Act 1998 and the General Data Protection Regulations 2018, between Stanley Group and any relevant third parties. I/We agree that Stanley Group, or any such third party may contact me in the future by any means of communication considered appropriate at the time.

If there is a means of communication that **YOU DO NOT** wish us to use, please indicate by ticking the appropriate box(es) below:

Post	☐	Telephone	☐	Email	☐	SMS	☐

Client Signature:	Client Signature:
Print Name:	Print Name:
Date of Signature:	Date of Signature:

DATA PRIVACY STATEMENT GLOSSARY OF TERMS

Glossary of Terms

We, us or **our**:	Stanley Group Consultants Ltd., 483 Green Lanes, Palmers Green, London N13 4BS
Contact information:	These are details that can be used to contact a person, including title, first name, surname, personal telephone number, fax, email address, home address, country, postcode or city of residence. This may also include work contact information such as work telephone number, fax, work email and work address.
Data Controller:	Means a natural or legal person (such as a company) which determines the means and purposes of processing of personal data. For example, *we* are your data controller as *we* determine how *we* will collect personal data from you, the scope of data which will be collected, and the purposes for which it will be used in the course of *us* providing you with *intermediary services.*
Data Protection Regulation:	Applicable data privacy and protection laws.
Employment Status:	This is information about your work, if you are employed, self-employed, unemployed, a student or on job seeker allowance.
FCA:	The Financial Conduct Authority, being the independent watchdog that regulates financial services.
Financial Information:	This is information relating to your financial status, including salary/income, outgoings/expenditure, secured and unsecured debt, tax rate and P60.
Health Information:	This is information relating to your medical history, including symptoms, diagnoses, procedures and outcomes, as well as information about your height and weight. This could include previous and current or persistent medical conditions and family medical history.
Identity Information:	This is any information that can be used to distinguish a person or verify their identity, such as name, date of birth, place of birth, gender, marital status, national identity card/number, passport, drivers' licence and national insurance number.
Intermediary Services:	These are the services we provide to you in relation to the products, which may include insurance products.
Lifestyle:	This includes both work and leisure.
Information:	Behaviour patterns. Most relevant to your *products* may be your smoker status, alcohol consumption, health, retirement age and exercise habits.
Product:	This is an investment, pension and/or protection product in respect of which we provide *intermediary services* to you.
Product Providers and Lenders:	A company which provides insurance, protection and/or general insurance products (**for a list of product providers which *we* work with, please contact *us* – see *How to contact us* above).**
Sanction Check Information:	This is information relating to your politically exposed persons (PEPs) status and Her Majesty's Treasury financial sanctions status, which is recorded to prevent fraud and money laundering.
Vulnerability:	A vulnerable person is someone who, due to their personal circumstances, is especially susceptible to detriment, particularly when a firm is not acting with appropriate levels of care. These persons are more likely to suffer severe detriment if something goes wrong. Details of vulnerability fall into the following categories: health; resilience (financial); life events; and capability (financial knowledge/confidence).

Stanley Group

Data Breach and Containment Policy

Contents Page

1 Introduction

1.1 The Data Protection Act 2018 (DPA) is based around six principles of 'good information handling'. These give people specific rights in relation to their personal information and place certain obligations on organisations that are responsible for processing it. An overview of the main provisions of DPA can be found in The Guide to Data Protection: https://ico.org.uk/for-organisations/guide-to-data-protection

1.2 Occasionally things will go wrong and mistakes will be made. Sometimes this may entail significant financial or reputational risk for businesses and staff. It is vital that we can identify, evaluate contain data breaches as soon as they occur.

1.3 Consistent governance and control arrangements are also a regulatory requirement. Where a breach has occurred and/or where you have failed to mitigate the impact quickly the Information Commissioner (ICO) may intervene and may use its powers to issue a substantial fine.

1.4 Identifying data breaches quickly and effectively to limit any impact on staff is critical to your success. Equally we need to understand where there are areas of weakness within our operating processes and continuously improve to reduce the risk of significant control failures leading to data breaches.

1.5 This policy meets the guidance provided by the ICO on data security breach management.

2 Aims and objectives

2.1 This policy sets out:

- Policy statement on data breaches
- Definitions
- Reporting responsibilities

2.2 This policy aims to ensure that adequate controls are in place so that:

- Data breaches are identified and action is taken quickly. Actions should be proportionate, consistent and transparent
- An assessment is completed to ensure that any major data breaches are reported to the Senior Management Team (SMT), Data Protection Officer (DPO) and the ICO appropriately
- All data breaches and near misses are recorded and regularly reported
- Lessons are learnt to ensure similar mistakes are not repeated and appropriate control mechanisms are put in place.

3 Policy Statement

3.1 This policy is in place to raise awareness of the risk of data breach. To ensure that all staff understand the steps required for dealing with them.

3.2 This policy identifies inherent risk of a data breach and/or near-miss, which will ensure that appropriate senior management and DPO are informed, able to manage actions relating to any real or potential serious data breach and be in a position to report to the ICO and affected individuals as appropriate.

4 Definitions

4.1 What is a data breach?

- According to the ICO organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.

- A data breach is “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”.

- A personal data breach may mean that someone outside the company gets unauthorised access to personal and/or special category (sensitive) data. But a personal data breach can also occur if there is unauthorised access within the company for example an employee accidentally or deliberately alters or deletes personal data.

A data security breach can happen for many reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it.

Human error is the most common cause of data breaches. These can happen for many reasons:

- Theft or loss of paperwork
- Data posted to incorrect recipient
- Data sent by email to incorrect recipient
- Failure to redact personal/sensitive data.

4.2 What is a near miss?

- A near miss is an event that does not result in a data breach, but which had the potential to do so. Examples of such events might include data that was misplaced but found quickly internally or data that was sent out but was identified and returned.

- Your company should be committed to identifying weaknesses in your operational procedures. You will record all near misses in order to understand patterns, learn lessons and implement improvements.

5 Training

5.1 Mandatory training will be provided to all staff on data protection regulations

5.2 Training will be provided to all new employees including temporary and contracted staff.

5.3 All employees will undertake refresher training annually

5.4 Your Data Protection Officer will receive training on data breach management and data breach reporting

6 Identification

6.1 Data breaches or near misses may be identified as part of everyday business.

6.2 Where a data breach is identified the company's designated member of staff and the Data Protection Officer must be informed immediately. The staff member (with support from the Data Protection Officer) will investigate the occurrence and complete a risk assessment (see the Risk Matrix) to determine the notification requirements.

6.3 The controls in place must be reviewed. Where no controls are in place, consideration must be given to introducing them. Was this an exceptional case that could not have reasonably been avoided, or does action need to be taken to avoid a recurrence?

7 Risk Assessments

7.1 When a data breach is identified a risk assessment should be completed using the Risk Matrix.

7.2 Depending on the risk assessment score the data breach will be reported to, owned and investigated at the specified levels within the company (see the Risk Matrix).

7.3 The DPO will be made available to support the data breach owner within the company. This officer will provide advice and guidance on managing the containment and recovery of any lost data and will support the investigation process. However, the data breach owner within the company will maintain overall ownership throughout.

7.4 The Data Breach Workflow should be used to work through the following stages.

NOTE: The relevant data breach owner should be notified immediately that a data breach has been identified or as a minimum within the timescales set out. This is a mandatory requirement. All incidents should also be reported to the Data Protection Officer who will decide how best to deal with the case. In some instances, investigations might be required to establish the scope of the issue identified.

8 Containment and recovery

8.1 Containment and recovery involves limiting the scope and impact of the data breach, and stemming it as quickly as possible.

8.2 The data breach owner, with support from the DPO, must quickly take appropriate steps to ascertain full details of the breach, determine whether the breach is still occurring, recover any losses and limit the damage. Steps might include:

- Attempting to recover any lost equipment or personal information
- Shutting down an IT system
- Contacting the Admin Office and other key departments so that they are prepared for any potentially inappropriate enquiries about the affected data subjects
- If an inappropriate enquiry is received staff should attempt to obtain the enquirer's name/contact details and confirm that they will ring the enquirer back
- The risk owner organising, with the approval of the Senior Management Team, for a company-wide email to be sent
- Contacting the Admin Office so they can be prepared to handle any press enquiries or to make any press releases
- The use of back-ups to restore lost, damaged or stolen information
- If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use
- If the data breach includes any entry codes or passwords then these codes must be changed immediately, and the relevant organisations and members of staff informed.

9 Investigation

9.1 If a data breach is identified, then a formal investigation should be commenced by the designated member of staff (data breach owner) who should determine the seriousness of the breach and the risks arising from it. Specifically, the data breach owner should identify:

- Whose information was involved in the breach
- What went wrong
- The potential affect on the data subject(s)
- What immediate steps are required to remedy the situation
- What lessons have been learnt to avoid a repeat incident.

In order to support this process the data breach owner should complete the Data Breach Report form.

9.2 The investigation should consider:

- The type of information
- Its sensitivity
- How many individuals are affected by the breach?
- What protections are in place (e.g., encryption)?

- What happened to the information?
- Whether the information could be put to any illegal or inappropriate use
- What could the information tell a third party about the individual?
- How many people are affected?
- What types of people have been affected (the staff, parents, staff etc)?
- Whether those affected have any special needs/vulnerabilities.

NOTE: Actions to contain and recover data as well as mitigate any risk should be taken immediately. The investigation is to ensure that the case is being managed and any improvement actions agreed are implemented. The investigation should be proportionate to the breach identified and risk of harm.

9.3 The initial investigation should be completed urgently and wherever possible within 24 hours of the breach being discovered / reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved

9.4 However, some level of investigation might be required to carry out the Risk Assessment and determine the most appropriate route of escalation. If, once identified, risk of a data breach is contained and does not pose immediate further threat to the company and/or staff, timeframes for official escalation/notification can be extended to allow for a more thorough investigation. Extensions must be agreed at each stage and noted in the report.

9.5 As an investigation proceeds the risk may change and the reporting requirements should be amended in line with the change in risk. For example, a case identified as a significant risk initially may increase to a major risk and therefore should be escalated to the ICO

9.6 Advice, input and support can be sought from your Data Protection Officer as required.

10 Informing affected individuals

10.1 The ICO requires us to inform those affected where there is a significant breach of personal and sensitive data and the risk of harm to those individuals is high.

10.2 Clearly if there was a high risk of further harm the company would have an obligation to disclose the breach to each individual affected. However, this has to be balanced against the risk of causing further distress and anxiety to the families by informing them about the breach.

10.3 The ICO guidance states that “informing people about a breach is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.”

10.4 Only the data breach owner and DPO can decide whether to advise affected individuals of a data breach and therefore the reasons for deciding to do this should be clearly set out in the investigation report and discussed with the data breach owner and other involved parties before affected parties are informed.

10.6 Further advice on whether to disclose to individuals is contained in the ICO Guidance on Assessing Disclosure to Individuals affected by a Data Breach.

11 Learning lessons

11.1 The Lessons Learnt Action Plan for data breaches and near misses should be completed and will form part of the investigation process.

11.2 The action plan should clearly outline the lessons learnt. The controls agreed to reduce the risk of a further reoccurrence, a lead member of staff and a completion date.

11.3 The case will not be considered closed until all actions agreed have been completed.

12 Performance monitoring and responsibilities

12.1 90% of investigations should be completed within 10 working days of the data breach being identified.

12.2 Where a major risk has been identified:

- An interim report should be presented to the Head / Governor a minimum within 10 working days even when the case cannot be concluded within this timescale
- Further reports should be presented to Governors at least every 10 working days until the case is concluded.

13 Information Governance

13.1 Information Governance is a resource that can be utilised to support investigations into identified data breaches. In any event, all data breach investigation reports should be shared with LBC's Information Governance Team or the DPO review post completion.

14 Data breach Log

14.1 All data breaches, including near misses, will be recorded on the data breach Log. All issues identified by the application of this policy will be recorded in the data breach log and categorised according to whether it is a data breach or near miss.

14.2 This information will be reviewed and analysed at least monthly to identify patterns and monitor the implementation of agreed service improvements.

14.3 The DPO will collate all data breach reports and will report trends and lessons learnt quarterly to Governors

15 Related documents

- Data Protection Policy
- Freedom of Information Policy
- Subject Access Request Policy
- Document Retention Policy
- Information Security Policy

Data Subject Access Request (SAR) Policy, Guidance and Request Template

Prepared By: Andrew Baker
Date: 28 Jan 2021

Approved By: John Watts
Date: 29 Jan 2021

Summary of Changes Since Previous Version: New Policy

Contents

GDPR –
Subject Access
Rights

1.0 Overview and Scope

This document applies to the employees, staff, workers and/or other individuals working or undertaking a role under or on behalf of the Stanley Group which consists of Stanley Group Consultants Ltd., ("SGC") including The Stanley Group Foundation ("SGF"). Stanley Group is a data controller in respect of all personal data it processes and SGF is a data controller in respect of the personal data it processes. When the terms 'we', 'us' or 'our' are used it should be read as referring to the Stanley Group, unless otherwise specified.

The General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 ("the 2018 Act") provide data subjects with a variety of rights in relation to the personal data held about them by Stanley Group. A summary of these rights are set out below.

It is important to note that data subjects have the right to appeal any decision made by Stanley Group in response to any data subject request to the Information Commissioner's Office ("ICO"). In the event the ICO finds that Stanley Group has infringed rights of a data subject, Stanley Group could be exposed to ICO action including a monetary penalty of the higher of 4% of Stanley Group's annual global turnover or €20M. Therefore, it is important that Stanley Group treats all individuals fairly and each data subject request is handled in accordance with this policy and legal requirements.

Members of staff etc. should consult Stanley Group's Information Governance Officer on info@stanleygroup.org if they receive a data subject right request.

The following definitions are applicable to this policy:

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

Special Category of Data: means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

For the purpose of this policy, when we are referring to 'personal data', we are referring to Personal Data and Special Category of Data collectively.

Overview of Rights of Data Subjects

Data Subject Rights include:

2.1.1 Right to be informed – data subjects have the right (subject to a few exceptions) to be provided with information on how their personal data will be handled by Stanley Group. Arts 12 – 14 of GDPR set out the information that must be provided and typically this information is provided by way of a privacy notice. Stanley Group has taken steps to meet its requirements in this regard by updating its employee privacy notice, PhD privacy notice and website privacy notice and will continue to monitor this issue to ensure the correct information is being given at the appropriate times. Please see Stanley Group Privacy Notice Policy and Guide if you feel a privacy statement is required.

2.1.2 Right of access to their personal data – the purpose of a subject access request is to allow individuals to confirm the accuracy of personal data and check the legality of processing to allow them to exercise rights of correction or objection if necessary. However, individuals can request to see any personal data that Stanley Group holds about them which includes copies of email correspondence referring to them or opinions expressed about them.

2.1.3 Right to Rectification - the right of individuals to require Stanley Group to rectify inaccuracies in personal data held about them. In some circumstances, if personal data is not complete, an individual can require the controller to complete the data, or to record a supplementary statement.

2.1.4 Right to be forgotten (erasure) – Individuals have the right to have their data erased in certain situations such as where the data is no longer required for the purpose for which it was collected, the individual withdraws consent, the individual has objected to processing based on legitimate interests, public task or official authority or the information is being processed unlawfully. There are certain exemptions to this right and there is no absolute obligation on Stanley Group to erase the relevant data – it is important to identify whether any exemptions apply.

2.1.5 Right to Restriction - Individuals can ask Stanley Group to 'restrict' processing of the personal data whilst complaints (for example, about accuracy) are resolved. Individuals can also ask Stanley Group to restrict processing where the processing is unlawful, Stanley Group no longer needs the personal data but the individual does not want it erased and/or the individual has objected to the processing and while the objection is

being considered, the individual wishes their data restricted.

2.1.6 Right to Portability – the data subject has the right to request that personal data concerning them and held by Stanley Group is provided to the individual (or a third party) in a structured, commonly used and machine-readable form. This right only applies to personal data that is processed by automated means (not paper records) and the processing is based either on consent or contract.

2.1.7 Right to Object – data subjects have the right to object to specific types of processing based on (i) public interest/official authority; or (ii) legitimate interests; or where it involves processing for direct marketing. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation except in the case of direct marketing where it is an absolute right. If Stanley Group receives an objection to direct marketing, it must stop processing the personal data for this purpose immediately. Otherwise, Stanley Group is entitled to consider whether there is legitimate grounds for the processing which overrides the interests, rights and freedoms of the data subject or whether it needs to process the personal data for the establishment, exercise or defence of legal claims; in both cases Stanley Group can override the objection.

2.1.8 Rights in relation to automated decision making and profiling – the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. "Profiling" is the processing of data to evaluate, analyse or predict behaviour or any feature of their behaviour, preferences or identity. The foregoing right does not apply if: (a) it is necessary to enter into a contract with the data subject and Stanley Group; (b) it is authorised by applicable law (and such law lays down suitable measures to safeguard the data subjects rights and freedoms and legitimate interest) or (c) is based on the data subject's explicit consent. However, even if (a) or (c) is relevant, please note that Stanley Group must put in place suitable measures to safeguard the rights of the data subject including the right to ask for a human to review the decision on behalf of Stanley Group and to contest the decision. Further, automated decision-taking based on special category of data can only be done with explicit consent.

3. Response Procedure

3.1 General:

a) Communication:- any communication with the data subject when responding to any request must be in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Communication should be in writing or by other means if appropriate
e.g. electronic means. It can also be provided orally if requested by the data subject, provided that Stanley Group is satisfied of the identity of the data subject and this is proven by other means. Where the request is by electronic means, the information should be provided electronically where possible, unless otherwise requested by the data subject;

b) Timing: - any requests made to invoke any of the rights above must be dealt with

promptly and in any case within one month of receiving the request. There may be some circumstances where Stanley Group can take longer than one month to fulfil the request (up to a maximum two further months where the request is complex or high number of requests being dealt with) however these are limited and Stanley Group should always strive to meet the

one month timeframe wherever possible. If Stanley Group needs to extend the response deadline, it must inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay;

c) Costs - in most circumstances Stanley Group will not be able to charge a fee for responding to any data subject request, unless the requests are manifestly unfounded or excessive in particular because of their repetitive character. In this case, Stanley Group will have to demonstrate how the request is manifestly unfounded or excessive in character and can either charge a reasonable fee taking into account the administrative costs of providing the information or communication, taking the action required or refuse to act on the request.

3.2 Step One: - Stanley Group should acknowledge receipt of a data subject request and confirm that Stanley Group is looking into the request and will respond within the statutory timeframe. Our letter acknowledgment template can be found at Appendix 1 of this Policy and must be used in response to each data subject request.

If Stanley Group has concerns over the identity of the natural person making the request, Stanley Group may request the provision of additional information necessary to confirm the identity of the data subject, which has the effect of 'stopping the clock'. Stanley Group would not be obliged to respond to the request until it is satisfied of the identity of the person (acting reasonably). Please note it is possible that Stanley Group may receive requests for a third party on behalf of a data subject e.g. a solicitor or a power of attorney or a friend.

In these cases, Stanley Group needs to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

If Stanley Group is of the view that the data subject may not understand what information would be disclosed to a third party who has made a subject access request on their behalf, Stanley Group may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it. In many respects, this would be the safest option for Stanley Group in this scenario.

3.3 Step Two: - assess whether Stanley Group requires to extend the deadline to respond to the request and/ or whether it needs additional information before responding and communicate this to the data subject as soon as possible and no later than one month following receipt of the request.

3.4 Step Three: - identify relevant personal data. This can take some time to accumulate therefore it is recommended to start the process as soon as possible following Step Two.

3.5 Step Four: - identify whether any exemption applies. It is important to remember that there are circumstances where Stanley Group would not require to comply with the data subject's request as referred to above in the explanation of the rights. There are also further exemptions set out in section 15 of the 2018 Act. Each request should be considered on its own merit and

in relation to the facts and circumstances at the time. Basic information on the exceptions to the above data subject rights can be found at https://ico.org.uk/for-organisations/guide-to- the-general-data-protection-regulation-gdpr/individual-rights/ The 2018 Act is a complex piece of legislation and provision of detailed explanation of exemptions is out side the scope of this policy. The Responsible Person should consider the detail of exemptions carefully. Please also see section 5 of this policy for guidance.

3.6 Step Five:

a) (Scenario A): - if, having considered the data subject request, Stanley Group decides not to comply in full because an exemption applies, an explanation must be provided to the individual within the deadline, informing them of their right to complain to the ICO and their right to seek a judicial remedy;

b) (Scenario B): - if, having considered the data subject request, Stanley Group decides that an exemption does not apply at all, Stanley Group must comply with the request and confirm compliance/disclose the relevant information within the statutory timeframe as above;

c) (Scenario C): - if, having considered the data subject request, Stanley Group decides that an exemption applies in part, it should communicate to the data subject within the statutory timeframe its response and where the request is a data subject access request provide the necessary information with the non-disclosable information redacted where appropriate. The data subject should be informed of their right to complain to the ICO and their right to seek a judicial remedy.

3.7 Step Six: Tracking Requests and Responses: - data subject requests must be tracked and recorded by Stanley Group for accountability purposes.

4. Subject Access Request Procedure

4.1 All Subject Access Requests received by Stanley Group will be processed by the Information Governance Officer (IGO). Any requests received by Stanley Group staff should be e-mailed to the IGO (info@stanleygroup.org) without delay in order that a response can be issued within the statutory deadline of one month.

The right to access their personal data is one of the most likely forms of subject requests Stanley Group will receive. The above information applies equally to data subject access requests. However it should be noted that when responding to data subject access requests, data subjects are also entitled (unless an exemption applies) to be informed of the following:

a) Confirmation that personal data about them is being processed.

b) A copy of that personal data.

c) Details of the purpose of the processing.

d) Categories of the personal data concerned e.g. does it include any special categories or sensitive personal information.

e) Any recipients or categories of recipients the personal information has been shared with, particularly if these are situated or domiciled outside the EU.

f) What safeguards are in place for transfers out with the EU.

g) The period the personal information will be stored for or what the criteria are for determining the period of storage.

h) The existence of the right to request from the data controller the correction or deletion of personal data or to restrict or object to the processing of personal data concerning them.

i) The right to lodge a complaint with the Information Commissioner's Office.

j) The source of the personal data if it has not been collected directly from the data subject.

k) Details of any automated decision-making, including profiling, and meaningful information about the logic involved and the envisaged consequences of such processing for the data subject.

4.2 As above, each data subject access request should be reviewed on its own merit and each time, Stanley Group should consider whether an exemption to disclosure applies. Section 15 of the 2018 Act sets out when organisations may refuse in whole or in part a data subject access request and information can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data- protection-regulation-gdpr/individual-rights/right-of-access/ As a general rule however, personal data relating to other individuals should not be disclosed (unless their permission has been obtained to release it or it is reasonable to comply without consent), therefore if this is within the requested information, Stanley Group should generally redact such information.

5. Exceptions to the Data Subject Rights

5.1 Section 15 of the 2018 Act sets out the exceptions to the rights vest in data subjects. The applicability of these should be reviewed on a case by case basis and it can be a complex area of law. Where appropriate, legal advice ought to be obtained. In summary, the main exceptions likely to be applicable include for reasons related to:-

a) Protecting the personal data of third parties;

b) Legal professional privilege;

c) Prevention or detection of crime;

d) Apprehension or prosecution of offenders;

e) Assessment or collection of tax or duty;

f) Immigration;

g) Information required to be disclosed by law or in relation to legal proceedings.

Appendix 1: Acknowledgment of Data Subject Request Letter Template

[DATA SUBJECT NAME/REQUESTER
NAME] [ADDRESS LINE 1]
[ADDRESS
LINE 2]
[POSTCODE/CI
TY] [COUNTRY]
[DATE]
Dear [DATA SUBJECT NAME/REQUESTER NAME]:

Reference: [DATA SUBJECT REQUEST TYPE/REFERENCE NUMBER]

We write to acknowledge receipt of your request dated [DATE] made under Article [NUMBER] of the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR). We received your request on [DATE].

The GDPR requires us to respond to requests within one month of receipt. We expect to provide a response by [DATE]. However, in certain circumstances, the GDPR or other applicable law allows us to extend that deadline by two months depending on the complexity of your request. We will advise you within one month if we need to extend the response deadline.

Our initial response letter may also advise you that:

We require more information to verify [your identity/your legal authority to make the request on another individual's behalf].

We need more information to respond to the request.

We require you to pay a fee before we respond to the request.

If we cannot honour the request, we will inform you of the reasons why, subject to any legal or regulatory restrictions by [DATE].

If you have any questions on the status of the request, please contact [NAME AND TITLE] at [TELEPHONE NUMBER] or [EMAIL ADDRESS]. [To check the status of the request, you may also use [our secure portal/[SUBMISSION MECHANISM]], after authenticating your identity with your [username and password/[OTHER AUTHENTICATION MECHANISM]].]

Sincerely,

_____

[SENDER NAME] For and on behalf of [Stanley Group / Stanley Group Foundation]

Appendix 2: Data Subject Access Request Form

Stanley Group
[Institute/Limited] Data
Subject Access Request
Form

Article 15 of the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) grants you the right to access your personal data held by [Stanley Group] or [Stanley Group Foundation], including the right to obtain confirmation that we process your personal data, receive certain information about the processing of your personal data, and obtain a copy of the personal data we process. We request that you submit this electronically via email to our Information Governance Officer at info@stanleygroup.org. Please note use of this form is not mandatory and you may submit your request in other formats e.g. plain email if that is preferable.

We expect to respond to your request within one month of receipt of a fully completed form and proof of identity.

I. Requester Name (Data Subject) and Contact Information

Please provide the data subject's information in the space provided below. If you are making this request on the data subject's behalf, you should provide your name and contact information in Section III.

We will only use the information you provide on this form to identify you and the personal data you are requesting access to, and to respond to your request.

First and last name:	
Any other names that you have been known by (including nicknames):	
Home address:	
Date of birth:	
Telephone number:	
Email address:	
If you are a current or former employee of Stanley Group please provide your employee identification number and your approximate dates of employment:	

Please provide other unique identifiers or related information to help us locate your personal data (for example, government identification number or customer account number):	

[II. Proof of Data Subject's Identity

We require proof of your identity before we can respond to your access request. To help us establish your identity, you must provide identification that clearly shows your name, date of birth, and current address. We accept a photocopy or a scanned image of one of the following as proof of identity: passport or photo identification such as a driver's license, national identification number card, or birth or adoption certificate. If you have changed your name, please provide the relevant documents evidencing the change.

If you do not have any of these forms of identification available, please contact Stanley Group for advice on other acceptable forms of identification.

We may request additional information from you to help confirm your identity and your right to access, and to provide you with the personal data we hold about you.

[III. Requests Made on a Data Subject's Behalf

Please complete this section of the form with your name and contact details if you are acting on the data subject's behalf.

First and last name:	
Home address:	
Date of birth:	
Telephone number:	
Email address:	

We accept a photocopy or a scanned image of one of the following as proof of your identity: passport or photo identification such as a driver's license, national identification number card, or birth or adoption certificate. If you do not have any of these forms of identification available, please Stanley Group for advice on other acceptable forms of identification. We may request additional information from you to help confirm your identity if necessary.

We also require proof of the data subject's identity before we can respond to the request. To help us establish the data subject's identity, you must provide identification that clearly shows the data subject's name, date of birth, and current address. We accept a photocopy or a scanned image of one of the following as proof of identity: passport or photo identification such as a driver's license, national identification number card, or birth or adoption certificate. If the data subject has changed their name, please provide the relevant documents evidencing the change.

We accept a copy of the following as proof of your legal authority to act on the data subject's behalf: a written consent signed by the data subject, a certified copy of a Power of Attorney, or evidence of parental responsibility.

We may request additional information from you to help confirm the data subject's identity. We reserve the right to refuse to act on your request if we are unable to verify your legal authority to act on the data subject's behalf.

IV. Information Requested

To help us process your request quickly and efficiently, please provide as much detail as possible about the personal data you are requesting access to. Please include time frames, dates, names, types of documents, file numbers, or any other information to help us locate your personal data.

For example, you may specify that you are seeking:

Employment records or personnel records.

Personal data held by a specific department of
Stanley Group Medical records.
E-mail or other electronic communications (specify the approximate dates and times). Billing information.
Photographs.

Video footage.

User activity
logs.

Transaction histories

Correspondence between [NAME] and [NAME] between [DATE] and [DATE].

We will contact you for additional information if the scope of your request is unclear or does not provide sufficient information for us to conduct a search (for example, if you request "all information about me"). We will begin processing your access request as soon as we have verified your identity and have all of the information we need to locate your personal data.

Description of Data Requested

If the information you request reveals personal data about a third party, we will either seek that individual's consent before responding to your request, disclose it, or we will redact third parties' personal data before responding. If we are unable to provide you with access to your personal data because disclosure would violate the rights and freedoms of third parties, we will notify you of this decision.

Applicable law may allow or require us to refuse to provide you with access to some or all of the personal data that we hold about you, or we may have destroyed, erased, or made your personal data anonymous in accordance with our record retention obligations and practices. If we cannot provide you with access to your personal data, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

V. Signature and Acknowledgment

I,_____, confirm that the information provided on this form is correct and that I am the person whose name appears on this form. I understand that: (1) Stanley Group must confirm proof of identity and may need to contact me again for further information; (2) my request will not be valid until Stanley Group receives all of the required information to process the request; and (3) I am entitled to one free copy of the personal data I have requested, and acknowledge that for any further copies I request, Stanley Group may charge a reasonable fee based on administrative costs.

If you would like to receive a copy of the personal data you are requesting access to, please indicate below whether you would like a hard copy or an electronic copy:

☐ Hard copy.
☐ Electronic copy.

_____

Signature

_____

Date

[**VI. <u>Authorized Person Signature</u>**

I,_____, confirm that I am authorised to act on behalf of the data subject. I understand that Stanley Group must confirm my identity and my legal authority to act on the data subject's behalf, and may need to request additional verifying information.

_____

Signature

_____

Date]

Version Control

Title	Subject Access Request Policy, Guide and Template
Author/Creator	Data Protection Officer
Owner	Data Protection Officer
Date Published/Approved	
Version	FINAL.V1.{{DATE}}
Date of Next Review	
Audience	All Stanley Group Staff and Stakeholders
Related Documents	GDPR Policy
Subject/Description	Policy provides guidance and processes relating to the administration of Subject Access Requests.
Group	
Department	

Your Privacy

We take your privacy very seriously and *we* ask that you read this privacy notice carefully as it contains important information on who *we* are, how and why *we* collect, store, use and share personal data, your rights in relation to your personal data and on how to contact *us* and supervisory authorities in the event you have a question, concern or complaint.

Italicised words in this privacy notice have the meaning set out in the Glossary of Terms at the end of this document.

Who we are

Stanley Group uses and is responsible for the way in which we process, record and manage certain personal data about you. When *we* do so *we* are required to comply with *data protection regulation,* and *we* are responsible as a *data controller* of that personal data for the purposes of those laws.

We are a company whose office is at 483 Green Lanes, Palmers Green, London N13 4BS, United Kingdom of Great Britain and Northern Ireland.

The personal data we collect and use

In providing our service to you *we* may collect the following personal data when you provide it to *us*:

- *Your contact information,* including name, address, telephone and email address information
- *Your identity information*, including date of birth, passport and driving licence details, National Insurance number, address verification (e.g. utility bills) and any other identify information we are required to collect within jurisdiction in which you reside or in which we operate or provide services on your behalf
- *Financial information,* including your income and expenditure, property, investments and information about other assets, and any mortgage loans and other secured and unsecured loans and credit cards
- *Your employment status*
- *Information about your lifestyle, for example nicotine and/or alcohol consumption*
- *Health information*
- *Details of any vulnerability*
- *Details of your dependents and/or beneficiaries under a policy* ***(If you are providing information about another person, we expect you to ensure that they know you are doing so and are content with their information being provided to us. You might find it helpful to show them this privacy notice and if they have any concerns please contact us in one of the ways described below.)***
- *Information about any existing business interests and/or potential conflicts of interest*
- *Criminal and background checks, where we are required to obtain and record this information, for example in matters of employment*

Information collected from other sources

We also obtain personal data from other sources in providing our *intermediary services*. Where *we* obtain this information from another party it is their responsibility to make sure they explain that they will be sharing personal data with *us* and, where necessary, ask permission before sharing information with *us*.

The personal data *we* obtain from other sources may include the following:

- From identification and verification checking agencies:
  - *identity information*
  - *sanction check information*
- Solicitors and accountants:
  - Details of wills and/or Trusts
  - Business accounts

Personal data (shown in table)

- How *we* use your personal data
- The lawful bases upon which *we* collect and use your personal data
- With whom *we* routinely share your personal data

Rationale/Reason for Processing	Lawful Basis for Processing	Third party recipients linked to that activity
To provide you with intermediary services	Performance of a contract Consent for special categories of data	Our clients, product providers and consultants
To submit tenders for services or participation in arrangement of contractual obligations	Performance of a contract Consent for special categories of data	Our clients, product providers and consultants
To retain records of any services or advice provided to you by us in order to defend legal claims or complaints	Legitimate interests	External suppliers of data storage and data hosting services to retain records on our behalf.
To provide you with details of products and services from us and third parties that may be of interest to you in accordance with your preferences.	Consent	

Special category data

Certain types of personal data are considered more sensitive and so are subject to additional levels of protection under data protection legislation. These are known as 'special categories of data' and include data concerning your health, racial or ethnic origin, genetic data and sexual orientation. Data relating to criminal convictions or offences is also subject to additional levels of protection. *We* may process:

- *health information* and *lifestyle information* when providing *intermediary services* in relation to a protection insurance product for the purposes of services supply to our clients or Group projects/programmes of work

In addition to the lawful basis for processing this information set out in the above table, *we* will be processing it either (i) for advising on, arranging or administering an insurance contract or (ii) for the establishment, exercise or defence of legal claims.

Whether information must be provided by you, and if so why

We will tell you if providing some personal data is optional, including if *we* ask for your consent to process it. In all other cases you must provide your personal data for *us* to provide you with *intermediary services*.

How long your personal data will be kept

We only retain your data for so long as it is necessary to fulfil the purpose for which it was collected. There are regulatory and legislative requirements which oblige us to keep certain data for longer, and to comply with those regulatory requirements we keep that data for seven years. In very limited circumstances, we may be required to keep some specific information for longer, but we regularly review our retention obligations to ensure we don't keep personal information longer than we are legally obliged to.

If you want details of the statutory retention periods for various product types, please contact us and we will obtain the latest legal position on your behalf.

Transfer of your information out of the EEA

We will not transfer your personal data outside of the European Economic Area. However, product providers, lenders and investment managers may administer your data and/or policy, as well as any existing contract(s) for services you may have with them for the provision of other services, from centres in countries outside Europe (such as India and the USA). Such countries do not have the same data protection laws as the United Kingdom or the EEA. However, they are required to put into place a European Commission-approved contract that that will safeguard your privacy rights and give you remedies in the unlikely event of a security breach.

Your rights

You have legal rights under *data protection regulation* in relation to your personal data. These are set out under the below headings:

- To access personal data
- To restrict how *we* use personal data
- To object to how *we* use personal data
- To ask *us* to transfer personal data to another organisation
- To find out more about how *we* use personal data

We will ask you for proof of identity when making a request to exercise any of these rights. *We* do this to ensure *we* only disclose information or change your details where *we* know *we* are dealing with the right individual.

We will not ask for a fee, unless *we* think your request is unfounded, repetitive or excessive, or the data request is complex, or you ask for multiple copies of the same information. Where a fee is necessary, *we* will inform you before proceeding with your request. We withhold the right to decline your request where we are authorised by regulation and/or legislation to do so.

We aim to respond to all valid requests within one month. It may however take us longer if the request is particularly complicated or you have made several requests. *We* will always let you know if *we* think a response will take longer than one month. To speed up *our* response, *we* may ask you to provide more detail about what you want to receive or are concerned about.

We may not always be able to fully address your request, for example if it would impact the duty of confidentiality *we* owe to others, or if *we* are otherwise legally entitled to deal with the request in a different way.

To access personal data

You can ask *us* to confirm whether or not *we* have and are using your personal data. You

can also ask to get a copy of your personal data from *us* and for information on how *we* process it.

To rectify / erase personal data

You can ask that *we* rectify any information about you which is incorrect. *We* will be happy to rectify such information but would need to verify the accuracy of the information first.

You can ask that *we* erase your personal data if you think *we* no longer need to use it for the purpose *we* collected it from you.

You can also ask that *we* erase your personal data if you have either withdrawn your consent to *us* using your information (if *we* originally asked for your consent to use your information) or exercised your right to object to further legitimate use of your information, or where *we* have used it unlawfully or where *we* are subject to a legal obligation to erase your personal data.

We may not always be able to comply with your request, for example where *we* need to keep using your personal data to comply with *our* legal obligation or where *we* need to use your personal data to establish, exercise or defend legal claims.

To restrict our use of personal data

You can ask that *we* restrict *our* use of your personal data in certain circumstances, for example

- where you think the information is inaccurate and *we* need to verify it;
- where *our* use of your personal data is not lawful, but you do not want *us* to erase it;
- where the information is no longer required for the purposes for which it was collected but *we* need it to establish, exercise or defend legal claims; or
- where you have objected to *our* use of your personal data, but *we* still need to verify if *we* have overriding grounds to use it.

We can continue to use your personal data following a request for restriction where *we* have your consent to use it; or *we* need to use it to establish, exercise or defend legal claims, or *we* need to use it to protect the rights of another individual or a company.

To object to use of personal data

You can object to any use of your personal data which *we* have justified based on our legitimate interest if you believe your fundamental rights and freedoms to data protection outweigh *our* legitimate interest in using the information. If you raise an objection, *we* may continue to use the personal data if *we* can demonstrate that *we* have compelling legitimate interests to use the information.

To request a transfer of personal data

You can ask *us* to provide your personal data to you in a structured, commonly used, machine-readable format, or you can ask to have it transferred directly to another *data controller* (e.g. another company).

You may only exercise this right where *we* use your personal data to perform a contract with you, or where *we* asked for your consent to use your personal data. This right does not apply to any personal data which *we* hold or process outside automated means.

You can contact us for more information

If you are not satisfied with the level of information provided in this privacy notice, you can ask *us* about what personal data *we* have about you, what *we* use your information for, who *we*

disclose your information to, whether *we* transfer it abroad, how *we* protect it, how long *we* keep it for, what rights you have, how you can make a complaint and from where *we* obtained your data.

If you would like to exercise any of the above rights, please:

- email or write to our Data Protection Officer at info@stanleygroup.org or 483 Green Lanes, Palmers Green, London, N13 4BS;
- let us have enough information to identify you, e.g. name, address, date of birth;
- let us have proof of your identity and address (a copy of your driving licence or passport and a recent utility or credit card bill); and
- let us know the information to which your request relates.

Keeping your personal data secure

We have appropriate security measures in place to prevent personal data from being accidentally lost or used or accessed in an unauthorised way. *We* limit access to your personal data to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. *We* will notify you and any applicable regulator of a suspected data security breach where *we* are legally required to do so.

Our supervisory authority

If you are not happy with the way *we* are handling your information, you have a right to lodge a complaint with the Information Commissioners Office (ICO). It has enforcement powers and can investigate compliance with *data protection regulation* (www.ico.org.uk). We ask that you please attempt to resolve any issues with us before the ICO.

How to contact us

- Please contact our Data Protection Officer if you have any questions about this privacy notice, or the information we hold about you. If you wish to contact our Data Protection Officer, please send an email to info@stanleygroup.org or 483 Green Lanes, Palmers Green, London, N13 4BS;

Declaration

I/We consent for Stanley Group to hold and process My/Our personal data for the purposes of provision of Professional Services, and I/We authorise the transfer of personal information, on a confidential basis and in accordance with the Data Protection Act 1998 and the General Data Protection Regulations 2018, between Stanley Group and any relevant third parties. I/We agree that Stanley Group, or any such third party may contact me in the future by any means of communication considered appropriate at the time.

If there is a means of communication that **YOU DO NOT** wish us to use, please indicate by ticking the appropriate box(es) below:

Post ☐ Telephone ☐ Email ☐ SMS ☐

Client Signature:	Client Signature:
Print Name:	Print Name:
Date of Signature:	Date of Signature:

DATA PRIVACY STATEMENT GLOSSARY OF TERMS

Glossary of Terms

We, us or **our**:	Stanley Group Consultants Ltd., 483 Green Lanes, Palmers Green, London N13 4BS
Contact information: including title, first	These are details that can be used to contact a person, name, surname, personal telephone number, fax, email address, home address, country, postcode or city of residence. This may also include work contact information such as work telephone number, fax, work email and work address.
Data Controller: determines the means	Means a natural or legal person (such as a company) which and purposes of processing of personal data. For example, *we* are your data controller as *we* determine how *we* will collect personal data from you, the scope of data which will be collected, and the purposes for which it will be used in the course of *us* providing you with *intermediary services.*
Data Protection Regulation:	Applicable data privacy and protection laws.
Employment Status: self-employed,	This is information about your work, if you are employed, unemployed, a student or on job seeker allowance.
FCA:	The Financial Conduct Authority, being the independent watchdog that regulates financial services.
Financial Information: salary/income,	This is information relating to your financial status, including outgoings/expenditure, secured and unsecured debt, tax rate and P60.
Health Information: symptoms,	This is information relating to your medical history, including diagnoses, procedures and outcomes, as well as information about your height and weight. This could include previous and current or persistent medical conditions and family medical history.
Identity Information: person or verify their	This is any information that can be used to distinguish a identity, such as name, date of birth, place of birth, gender, marital status, national identity card/number, passport, drivers' licence and national insurance number.
Intermediary Services:	These are the services we provide to you in relation to the products, which may include insurance products.

Lifestyle: This includes both work and leisure.

Information: Behaviour patterns. Most relevant to your *products* may be your smoker status, alcohol consumption, health, retirement age and exercise habits.

Product: This is an investment, pension and/or protection product in respect of which we provide *intermediary services* to you.

Product Providers and Lenders: A company which provides insurance, protection and/or general insurance products (**for a list of product providers which *we* work with, please contact *us* – see *How to contact us* above).**

Sanction Check Information: This is information relating to your politically exposed persons (PEPs) status and Her Majesty's Treasury financial sanctions status, which is recorded to prevent fraud and money laundering.

Vulnerability: A vulnerable person is someone who, due to their personal circumstances, is especially susceptible to detriment, particularly when a firm is not acting with appropriate levels of care. These persons are more likely to suffer severe detriment if something goes wrong. Details of vulnerability fall into the following categories: health; resilience (financial); life events; and capability (financial knowledge/confidence).