douglas stafford®
GLOBAL

Approach Taken by Douglas Stafford to Achieve

GDPR COMPLIANCE

OVERVIEW

The General Data Protection Regulation comes into force on 25 May 2018 replacing the Data Protection Act 1998. It is largely the same, but has been strengthened in some areas, particularly with data that is being used to contact private individuals (as opposed to 'business to business').

Douglas Stafford is a recognised industry leader in providing a range of Performance Evaluation and Market Research services through Mystery Shopping Evaluation, (Video, Telephone, E-mail/Web, Social Media and Report Based), Audit and Housekeeping Services, Client Satisfaction Analysis and Client Contact Centre Initiatives, delivering solutions and know-how for business improvement. More information may be found on our website www.douglasstafford.com

The nature of Performance Improvement and Mystery Shopping services means that personal data will usually be processed in some way in order to meet the Client's objectives. This data would normally contain a person's name and contact details and as such would never normally be considered as sensitive data. Non-the-less this data needs to be processed in line with the GDPR regulation.

All our services are provided on the basis that the Client is the 'Data Controller' and Douglas Stafford is the 'Data Processor'.

Douglas Stafford have produced this document to not only explain what steps we have taken to ensure our processes and systems are fully GDPR compliant, but also to advise on how Douglas Stafford may help our Clients meet their Data Controller obligations with respect to data security matters. Please note this document is designed to cover those areas that effect on both Douglas Stafford and our Clients: It does not attempt to explain or advise on those areas where Douglas Stafford is the Data Controller (mainly personnel).

KEY POINTS TO ADDRESS

What is Personal Data? Broadly defined as a piece of information that can be used to identify an individual. Apart from more usual details such as name, contact details (many), gender, age, physical description, it also can include hand writing, an IP address, a voice message, visual data and video data.

Sensitive Personal Data: Additionally includes such information as religious, political or sexual orientation and details on pay, bank account, tax affairs and union membership etc. Sensitive data is never used or processed in support of the services that Douglas Stafford provides.

Express Permission to Contact: GDPR requires that you have obtained an Individual's express permission to contact them. An Individual has the right to request that they are permanently removed from a mailing/contact list and also to request sight of the data being held. GDPR focusses on an individual's rights and would not normally apply to bona fide business to business communication, however, we should still comply if a prospect or recipient requests that they wish to be removed from a marketing database. (The above contact removal applies to Telephone and Email only; from a GDPR/legal standpoint, it does not currently apply to postal communication).

DATA CATEGORISATION

A review of all data held and processed by Douglas Stafford has been carried out in order to establish whether we process the data as a Data Controller or Data Processor. In summary the results of the review are as follows:

Data Controller	Employee Records, Supplier Records and Marketing Database
Data Processor	Data used as part of providing our services to Clients

This data was further categorised into where it is stored, whether it is considered sensitive, who has access and what security has been applied. Our Security Policy was then reviewed to ensure that adequate and appropriate security has been applied.

DATA COMPLIANCE OFFICERS

As with all companies, the Directors have overall responsibility, however, they will not necessarily know what data has been received or is processed on a day to day basis. It was therefore decided to appoint two Data Compliance Officers. Both Officers will also be responsible for managing 'requests' received from affected individuals or recipients.

Data Compliance Officer – Operational: Responsible for managing the data that is received from Clients (and the manner by which it is received) and also the processing of this data that is subsequently carried out to fulfil our Clients' requirements.

Data Compliance Officer – Marketing: Responsible for managing the data that is used by the Sales & Marketing machine.

TERMS AND CONDITIONS

Douglas Stafford's standard terms and conditions have been updated to reflect the new GDPR requirement. In summary they confirm the basis on which we will process a Client's data, how we will support the Client in meeting their Data Controller obligations and how and when we will destroy the personal data at the end of the service agreement or before if it is no longer required. (Available upon request, see clause 13).

PRIVACY STATEMENT

All data collected and processed by Douglas Stafford, will be used strictly for the agreed purpose of providing the specified service to the Client and will never be used for onward dissemination to other non-related business parties. Data will be held in accordance with our Data Deletion Policy

In addition please note that:

- All Douglas Stafford employees and associated parties have signed a binding Confidentiality Agreement.
- All data, whether Personal or Business Contact, sent between Douglas Stafford and the Client will have appropriate levels of security applied.
- Douglas Stafford is registered with the Information Commissioners Office: Z8897183

SECURITY POLICY

Our Security Policy covers all aspects of security including the following areas:

- Security Policy Statement
- Data Protection Policy
- Physical Access
- IT System Security Policies and Access
- Equipment Disposal
- Employee Technology Usage Policy

The Security Policy has been updated as appropriate to meet the GDPR requirement. (Available upon request, see section 6.4, pages 7 & 8).

DATA DELETION POLICY

Douglas Stafford have produced a Data Deletion Policy that clarifies exactly how long different categories of data will be held. (Available upon request).

ADDITIONAL PROCESS required for GDPR COMPLIANCE

From both a Data Controller and Data Processor perspective, Douglas Stafford has established a **Robust and Auditable** process that will handle the following queries from a Data Subject:

- **Review** – data subjects have the right to see what personal data is held.
- **Correction** – if the data is proven to be wrong, it must be corrected.
- **Erasure** – a data subject can request that their name is removed from a contact list. Our process ensures that this is done permanently for the duration of the programme/contract and that we will inform the Data Controller/Client.

GDPR COMPLIANCE CLIENT SUPPORT

In addition to all of the above actions carried out by Douglas Stafford to ensure that we are GDPR compliant, we will support our Clients with the following activities:

- Notifying the Client of all access, correction and erasure requests received without undue delay.
- Assist the Client where practically possible in their obligation to respond to access requests.
- Reasonably support the Client to meet their Data Controller obligations with respect to data security matters.

GENERAL ADVICE & INFORMATION

The type of data held and used by Douglas Stafford would normally contain the following:

A. MYSTERY SHOPPING DATA
Name and business contact details (telephone, email and address)

B. CONTACT DATA
Name and private contact details (telephone, email and address)

This type of data would not normally be considered as '**sensitive**' however, there are a number of precautions that should be followed:

1. The file holding the information should be password protected prior to sending it to (and from) Douglas Stafford.
2. There should be an agreed timeframe in place for how long the 'data' will be held. Douglas Stafford's default policy on data storage, unless otherwise agreed with the Client, as follows:
    a. Contact data will be deleted immediately from our systems at the end of a project or project phase.
    b. Video data will be deleted 12 months after it was first published, or within 3 months of the end of the programme.
    c. Results data will be deleted after it is no longer being used by the Client.

GDPR COMPLIANCE & VIDEO MYSTERY SHOPPING

The introduction of GDPR does not really effect the laws and approach associated with Video Mystery Shopping.

- In the United Kingdom it is NOT illegal to video people or the general public and you do not need their express consent to do so. The BBC television news regularly feature members of the general public who are clearly identifiable to illustrate a general item of news.

- Most importantly (the key issue), the use of data of this nature (people on film) should not contain anything of a specifically personal nature that may be considered to be derogatory, demeaning or upsetting. For example, the BBC television news may comment on an increase in obesity and show some supporting 'public' footage. However in these instances, this footage will never show the identity of a person, as this would be considered to be derogatory, demeaning or upsetting.

- Video Mystery Shopping is standard practice in most market sectors in the UK, particularly in the Automotive and Retail industries, where it is used to support improved performance and Customer satisfaction, and the Banking and Finance sectors where it is additionally used to prove FCA 'compliance'.

- Whilst it is not a legal requirement, it is considered best practice to advise staff that a visual and audio evaluation programme may take place from time to time, and that they may be subject to Video and Audio recordings for the benefit of training and coaching purposes. Ideally this will be incorporated in the employee's Conditions of Employment or Staff Handbook, but it can also be done as a notification to all staff at the start of an evaluation programme. Douglas Stafford is happy to work with our Clients to produce an appropriate notification announcement.

- When Video Mystery Shopping data is used for the stated purpose, it does not normally matter whether members of the general public or other unrelated individuals were inadvertently caught on the film. However, as part of the quality control process, Douglas Stafford will not publish the results if they are felt to contain excess footage of children or anything that might be considered derogatory, demeaning or upsetting, particularly if the individual(s) might be known or recognised.

douglas stafford® GLOBAL