SAIF

GDPR Toolkit – Part One
General Data Protection Regulation (GDPR)

Introduction

On the 25th of May 2018 the European Union (EU) introduces the new data protection laws, which the United Kingdom (UK) is signed up to, irrespective of the decision to leave the EU. Therefore, the GDPR will supersede the current Data Protection Regulations of 1998.

The new regulations will impact every organisation in the UK that holds personal data of clients, customers, staff, volunteers and members. These regulations are far reaching and reflect the 'right to privacy' for the individual and each member of SAIF. Members needs to take the implications of these changes very seriously on how data is collected, recorded and stored (security and duration); and a clear authorisation of consent to retain data needs to be obtained.

We have found from the Isle of Man useful information that will help you prepare in the early stages in relation to data mapping. We have received permission to share this with our members.

SAIF will be issuing three GDPR Toolkits:
Part One – this release, end of November 2017.
Part Two – by early February 2018 (with supporting information from Golden Charter).
Part Three – by early April 2018, any final guidance received from the ICO.

Summary:

When are these laws effective from?	***25th May 2018***
Who will it impact?	***All organisations that retain personal information of others***

1. What your firm needs to do now?

A. Register your organisation with the Information Commissions Office (ICO)

To register your firm with the ICO costs £35 and a nominee from the office will be known as the "data controller". The data controller is responsible for the administration and oversight of all the firm's data and is the liaison point with the ICO and for your clients' requests for information.
Please note after 25th May 2018 it will not be necessary to register with the ICO as all compliance to GDPR will be mandatory, and inspections and audits by the ICO will occur randomly.
The ICO will be paying attention by scrutinising organisations that have 250 staff or more initially.

B. Encrypt your website coding.

The vast majority of SAIF member firms have a digital footprint, a website, which we thoroughly recommend as we engage the baby boomer, Generation Y and millennial generations, by whom 65% of decision making will be made via a website prior to any telephone or face to face conversation.

Please ensure your website uses encrypted coding. Your firm's Information Technology (IT) staff member or agent can achieve this usually without too much time.

The question you might ask is why should we do this, as you do not take payments or collect personal information from your website? Well, simply it is good practice in this era where data can be stolen via websites.

SAIF have a number of Associate Members who can support you and their details can be found on the inside rear cover of the SAIFInsight magazine, or please contact the SAIF Head Office for their details.

C. Map the Journey of how you collect Personal Information (data).

I. What client information do you collect and how do you store it?

It is important that your firm makes time between now and the end of January 2018 (suggested timeframe to give you space to make alternative arrangements) to map the journey of how client information and staff information is gathered, what information is held, and where it is safely stored.
For instance, if you store the data on a laptop (local drive storage), that you demonstrate a 'clear desk policy' at the end of every working day and the PC is stored ideally in a locked drawer. Furthermore, if you regularly back up this information that the external hard drive is securely locked away. Should you use 'cloud storage' that the information is encrypted and password protected and who in the firm holds those passwords.
If you collect data on paper records then these are likewise securely stored.

II. What data do you record and why?

The Part Two SAIF GDPR Toolkit (to be issued by beginning of February 2018) will include advice from Golden Charter on data protection guidance on funeral plans and direct marketing. Should you use another provider it is important you consult with their advisors.

For at-need clients the "arrangement form" is part of SAIF's Code of Practice, where information is collected, service needs documented and best practice states that this should be signed by the client.
We are consulting with our lawyers for additional clauses on this form to be included that allow for correct 'consent for information' to be added to the arrangement forms which will be signed and dated.

III. CCTV

If your premises use CCTV, there will be additional burdens for you in how you not only notify your clients, but how that video is stored. SAIF will be giving further guidance on this.

2. Staff and Third Party (Disbursement) Contractors

A. Staff – Employment Law

GDPR will affect what staff information you hold. There will be personal data from emergency telephone numbers, to financial and pension information, and performance management information.
When a staff member leaves, most of this information will need to be deleted, except for pension arrangements whilst in employment.
This information will require consent and be stored in secure places.

B. Clergy/Celebrants/Cemeteries and Crematoria

SAIF is consulting with celebrant organisations who are in Associate Membership as they will be required to meet the GDPR obligations.

Since clergy, celebrants, cemetery and crematoria authorities are contracted by the funeral director on behalf of your client, it will be important that these agents/contractors confirm they have satisfactory GDPR and retention of information policies in place. SAIF are consulting legal advisors for specific information that you will require that ensures you as funeral directors fulfil your duties placed upon your third party agents. These guideline notes will feature in Part Two.

C. Charity Donations in memorium

Many SAIF member firms already deploy Associate Member services where obituaries and/or online donation collections take the risk of cash completely away from the funeral director.

It is reasonable that if a firm still collects cash and cheques, it is able to pass forward to the charity on behalf of the client the details of the donor. We are consulting our legal advisors on this point, and certainly SAIF's view is that it is reasonable to pass onto the charity the name of the donor so that the charity can send an acknowledgement or a letter of thanks on behalf of the client's family. However, what would be a breach of GDPR is if the charity or funeral director marketed their organisations to the donor without explicit consent.

3. Privacy Notices, Retention Policies, Data Controllers, Processers and Subjects.

A. Privacy Notices

Whilst privacy notices are familiar below signatures on emails and statements on terms and condition documents, the GDPR elevates the importance of a 'right to be forgotten' element that is new to the new regulations.

Each firm will need to adopt a privacy notice that includes the firm's identity; the reasons for retaining personal data and how the organisation will process requests for data information by a client.

B. Data Controllers, Processers and Subjects

Data controllers are those responsible in your firm who are the point of contact for clients and the ICO and will manage the firm's data compliance.

Data processors can include other staff in the organisation as well as third party agents, such as celebrants.

Data subjects are clients whose personal data is held.

C. Data Protection Principles

There are eight data protection principles. These principles are to protect the interests of the individuals who personal data is being processed.

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be retained for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational (security) measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory (internationally) outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The GDPR gives strict guidelines for transparent processes for explicit consent by the data subject and timelines for

- A request for information by a data subject, which is 40 calendar days.
- Should there be a data breach, the data controller is to submit to the ICO within 72 hours of discovery setting out the breach and subsequent remedy.

Thought needs to be given how data subjects access their information, and what documentation you require signing and permissions should information of a client's next of kin form part of the data. SAIF will be seeking legal guidance to this, however, it is important to advise that each firm will need to be clear how it processes request for information, and thereby, it may be prudent to seek specific advice on your firm's unique set of criteria for operations.

4. Other Elements for Consideration

A. What about data prior to 25th May 2018

SAIF will confirm the guidance on this in Toolkit Part Two.

B. Retention Policy

SAIF will produce a template retention policy, however, it will be vital each firm's Data controller customises this according to your own control process of information.

C. Useful Information:

ICO

Irwin Mitchell LLP

SAIF Head Office