GENERAL DATA PROTECTION REGULATION (GDPR) FAQS

produced by...

National Association of Funeral Directors Est 1905

SAIF INDEPENDENT FUNERAL DIRECTORS

with thanks to...

Ecclesiastical PLANNING SERVICES

Golden Charter Smart Planning for Later Life

What is the difference between Data Controllers and Data Processors?

The Information Commissioner's Office's definition of controllers and processors is:

- A controller determines the purposes and means of processing personal data. For funeral plans that will be the plan provider.
- A processor is responsible for processing personal data on behalf of a controller. For funeral plans that will be the funeral director.
- If you are a processor, the General Data Protection Regulation places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.
- However, if you are a controller, you are not relieved of your obligations where a processor is involved – the General Data Protection Regulation places further obligations on you to ensure your contracts with processors comply with the regulation.

You are a data controller for your own business. If you offer pre-paid funeral plans, you will be a data processor for your plan provider.

What does it cost to register with the Information Commissioner's Office?

The cost of your Information Commissioner's Office registration depends on your size and turnover. There are three fee levels:

- You'll need to pay £40 if your business:
  - has a turnover of less than £632,000 per financial year; or
  - has fewer than 11 employees
- You'll need to pay £60 if your business:
  - has a turnover of less than £36 million per financial year; or
  - has fewer than 251 employees
- You'll need to pay £2,900 if your business:
  - has a turnover of more than £36 million per financial year; or
  - has more than 250 employees

You must tell the Information Commissioner's Office if you think your business should only pay the £40 or £60 fee – the presumption is that all data controllers are eligible to pay the £2,900 fee.

Some organisations only pay £40 regardless of their size and turnover. These are:

- charities;
- small occupational pension schemes; and
- organisations that have been in existence for less than one month.

Who is going to police the General Data Protection Regulation?

The Information Commissioner's Office will police the General Data Protection Regulation. Customers are encouraged to complain to the Information Commissioner's Office where they feel their information is not being handled correctly or they have not been able to access their information. This will inform the Information Commissioner's Office of issues in individual companies.

Are nationwide processes being put in place for local authorities (e.g. crematoria)?

This is not something that we are aware of and we encourage you to discuss this with your local crematoria.

What do ICO and DMA stand for?

Information Commissioner's Office and Direct Marketing Association.

When does the General Data Protection Regulation come into force?

25th May 2018.

Does the General Data Protection Regulation only affect registered companies and attributed associations?

The General Data Protection Regulation affects anyone/all companies who process personal data belonging to EU residents. It will still be applicable post-Brexit.

After a customer has passed away and the funeral is complete, can the funeral director contact the family to invite them to a bereavement service?

We reached out to the Direct Marketing Association and to our legal advisors for clarification on these types of services. Both the Direct Marketing Association and our legal advisor confirmed that they would deem this to be marketing as the funeral company may be trying to promote its services (whether in brand or promotion), and therefore consent is required. Consent should be captured at the time of arranging the funeral. Consent cannot be requested at a later date. Verbal consent is acceptable but must be recorded (name, date and time given) so it can be evidenced and edited if required.

After the funeral is complete, can the funeral director include a pre-need/ funeral plan promotional leaflet in with the invoices?

Consent would be required to do this – see previous question with regards to capturing consent.

Can funeral directors use old data to market to customers where no consent has been captured to do so?

Companies will not be able to contact customers to market to them after 25th May 2018 where no marketing consent (which is in line with the new regulation) has been gained.

Can funeral directors capture customer consent when arranging a funeral?

Yes.

If funeral directors forward donations on behalf of a client to a charity, can they give the charity the name and address of the person who has requested this, i.e. the next of kin or person arranging the funeral, thereby confirming that donations have been received?

If funeral directors are forwarding donations to a charity as part of the service agreed with customers, they can forward next of kin (NOK) details if this is made clear in the Privacy Notice and the customer has consented to their details being shared. The NOK or client cannot give permission on behalf of funeral attendees to share their data with charities.

Can I share the list of funeral attendees with the person organising the funeral?

If you wish to share a list of funeral attendees with a family, attendees need to know what their data is being captured for and who it will be shared with.

The annual remembrance service is essentially a marketing tool we use to promote our business. Although we do not promote or sell products, it is marketing nevertheless?

Yes. The Direct Marketing Association would deem this to be marketing.

Will we be able to contact NOK for marketing purposes?

If you have gained General Data Protection Regulation compliant consent directly from the NOK at the time of arranging the funeral you can contact them. If no consent is gained, unfortunately you cannot contact them to market to them.

Can funeral directors pass customer data to potentially non-compliant third parties where the customer says this is okay (e.g. an individual celebrant)? How would a funeral director know if they are compliant?

It is the funeral director's responsibility to ensure anyone they are passing customer information to is compliant with the law. You can ask the individual what their process for handling customer personal information is. You should also detail to the third party that the data should be used only for the intended purpose, held securely and destroyed once no longer required.

The DMA has confirmed that funeral directors would not need a data processing agreement for each individual or business whose services they engage for the purpose of carrying out a funeral, as:

1) The deceased person has no data protection rights as they are not a living individual

2) The personal details of the next of kin are passed on to celebrants, crematoria and cemeteries on a one time use basis only and only for the limited purpose of organising the service or cremation/ burial.

Would it be the celebrant's responsibility to delete the client's information or would it be the responsibility of the funeral director?

The funeral director should make the celebrant aware that they should not keep the customer data longer than necessary.

If a funeral director holds information on a PC or database, is there a specific malware or virus protector that should be used?

The General Data Protection Regulation outlines that companies should take appropriate measures to ensure the security of the customer information that they hold. This may vary across different businesses as each business will have a different set up and technology. The Information Commissioner's Office previously provided guidance to allow small businesses to determine what their own requirements were – A Practical Guide to IT Security. The Information Commissioner's Office have updated their guidance on security under the General Data Protection Regulation.

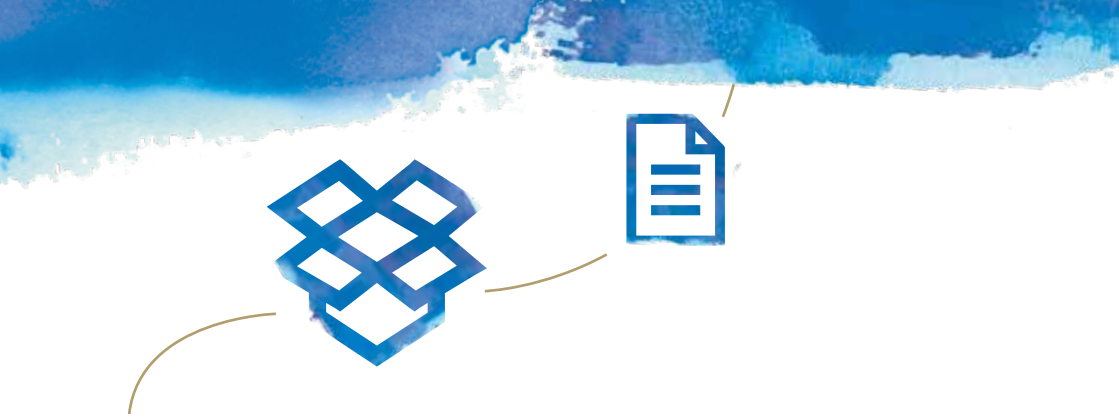
You should also be aware of the Privacy and Electronic Communications Regulation (PECR) 2003 – more information can be found at www.ico.org.uk/for-organisations/guide-to-pecr

Will funeral directors have to destroy old records?

The General Data Protection Regulation only applies to living individuals, therefore it depends on what information is held (living NOK, etc.) you may feel that it is reasonable to keep details for:

- Regular use of archived records for reference purposes at the request of next of kin or a future funeral arranger
- Future requests to exhume the remains of a deceased person, including cremated remains

You must document your reasons for holding data in your data processing summary statement (which should be given to clients at the earliest reasonable opportunity), privacy notice and document retention policy.



Can funeral directors use data backup sites such as Dropbox?

Funeral directors can use various sites to back up data as long as the site has appropriate security measures and is compatible with the General Data Protection Regulation. Individual sites will be able to give you further information on their adherence to the new regulation. You are responsible for that data and what happens to it. You should ensure that you do not use any backup sites that do not adhere to GDPR.

Can funeral directors include a data use policy within their terms of business or terms and conditions?

A privacy notice (or privacy policy or data use policy as it can also be known as) should be concise, transparent, intelligible and easily accessible. A privacy notice can be detailed within terms and conditions; however it must be made clear within the document. It should be noted that if a funeral director has a website that the privacy notice should be added to the website.

What happens if a family wants a funeral director to destroy data that we are legally obliged to keep for a specific time period?

The funeral director has a right to refuse a request to erase data where they must keep the data to comply with a legal obligation. However, the funeral director should consider WHAT information needs to be kept as it would be unreasonable to refuse to erase data if all that the funeral director required was a basic invoice and reference number. An example of what you may keep would be records required for tax purposes.

How would a funeral director record the shredding of paperwork?

It is important to keep an audit trail of what is deleted and when. A certificate of destruction and document retention policy will assist with ensuring you have an embedded process.

How much information can a funeral director give families of a recently deceased person without breaching the General Data Protection Regulation?

The General Data Protection Regulation only applies to living individuals, however you may wish to respect the wishes of the deceased and speak only to the plan representative and/or NOK. Once you have established that the customer has passed away you are free to share the customer information with the family. This would be the case for at-need and pre-need funerals. It should be noted that you cannot share plan representative or NOK details.

Will the General Data Protection Regulation affect online tribute pages?

The General Data Protection Regulation only applies to living individuals, and therefore information on the deceased can be shared online (as long as it does not affect living individuals, e.g. family members). Online tribute pages should contain a privacy notice and cookie policy.

Do I need a data processing contract with the providers that provide my software, call answering service and bookkeeping?

It would be advisable to cover their data processing obligations within the standard contract that you have with them.

If the celebrant chooses to contact the family after a month or longer time period to check how they are doing, do they need consent from the family to do this?

Yes. The celebrant would require consent (or another legal basis) to contact the family for marketing purposes after the contract is complete, i.e. the funeral service has been conducted.

Can I put general terms into a contract with my celebrants to get them to agree to delete data after a set period of time, rather than contact them after each service?

Yes. It would be advisable that where you have an ongoing relationship with a third party (which could be a celebrant, crematorium, etc.) to include all of the standard conditions you would expect them to adhere to within a contract. This may include a provision that they delete all personal data relating to a customer a set period after the service has been conducted. You may wish to review this contract and have it signed annually to ensure it remains relevant. You should have the ability to review their processes if required.

Can I keep customer details on documents I must retain for another purpose, e.g. HMRC records I must keep for seven years?

You should only retain information as long as is necessary. It is unlikely to be necessary for you to retain customer information for the purposes of a tax return. Data retention policies should be included in your privacy notice. The lawful basis for processing data can be found at www.ico.org.uk by searching 'lawful basis for processing'.

When can I keep NOK details?

You can keep NOK details for as long as is necessary, but is up to your business to determine what is 'necessary'. A funeral director recently advised the Information Commissioner's Office that it is necessary for them to retain NOK details in case a body is exhumed and they are obliged to notify the family, and the Information Commissioner's Office have agreed that this would be a legitimate reason for retaining NOK details indefinitely. This would be documented in the funeral director's retention policy and privacy notice.

Will the GDPR affect the way I can process information acquired prior to May 25th?

Yes. The collection date is not relevant. After 25th May 2018 it must be processed, stored and deleted in line with GDPR.

How long will I be able to hold client/ funeral records in future?

This will be determined by your retention policy.

How long will I be able to hold the personal information of my staff?

This will be determined by your retention policy. You should refer to employment law, for example there are specific rules around how long data should be retained for pension purposes. You need consent to hold CVs of job applicants that are unsuccessful.

We have kept historic records of every funeral we have carried out for generations, do I need to destroy these?

You can retain information relating to deceased persons. Consent is required to retain details of living persons after the funeral.

Do I always need to seek my client's consent to process their personal information?

Information must be processed in line with the lawful basis under GDPR. The lawful basis for processing data can be found at www.ico.org.uk by searching 'lawful basis for processing'.

Will I still be able to take a record of attendees at a funeral service?

Only if you are telling them what you will do with the data.

Will I still be able to provide a visitor book service?

The family should write in the first page and funeral attendees should know what will happen to the information. The funeral director cannot use this information for marketing/testimonial purposes unless they have consent from individuals to use it for marketing purposes.

Do I need to take down historical invoices that are currently displayed in my funeral home?

If any of the data subjects mentioned are still alive, you need their consent to continue to display these, otherwise they will have to be taken down.

Can I obtain consent for marketing by simply including a statement in my standard business terms?

You can ask for verbal consent, for example at the time of arranging the funeral, but you need to ensure this is documented including name, address, nature of consent, date and time given, so that the consent can be evidenced and edited if required. It must be held and destroyed securely. Consent cannot be obtained at a later date. As mentioned above, it needs to be captured at the time of arranging the funeral. Consent for marketing purposes must be separate from your standard business terms.

What is the difference between the Data Protection Act and the GDPR?

GDPR supersedes the Data Protection Act 1998 and gives more rights to individuals.

What is a subject access request and what should I do if I receive one?

Under GDPR anyone can request a copy of the data you hold on them. You should have a policy in place. You have 30 days to respond.

Do I need to have a data policy?

You should inform data subjects what information you hold and how you will use it. As a minimum you should have a data processing summary statement (sometimes referred to as a fair processing notice – this should signpost to your privacy notice), a privacy notice (i.e. a data policy), a data processing map (see the data processing map, which has been made available to NAFD and SAIF members), a retention policy, a subject access request policy, right to be forgotten process and data breach process. Information on what should be included in a privacy notice can be found on the ICO website – visit www.ico.org.uk and search 'privacy notice'.

What is a data breach and what should I do if I become aware of one?

You should have a data breach policy in place. There is a wealth of information on data breaches on www.ico.org.uk - simply search 'personal data breach'.

At what point do I need to provide details of our data processing approach? Do we need a recorded message on our phones or can this wait until the funeral arrangements are made? We may receive telephone calls from families who are recently bereaved and it may not be appropriate to provide this information on first contact?

It is acceptable to provide information on how you process data during an arrangement rather than on an initial call, where it may be inappropriate to do so particularly if the caller has been very recently bereaved. However, you should provide a copy of your summary data processing notice (sometimes referred to as a fair processing notice) which should include a link to your privacy notice (which can be online or available as a hard copy on request) as soon as possible.

You need to provide a data protection statement before capturing information, and this must capture consent to process Special Category Data and/or consent to use the data for marketing purposes if you plan to use it in this way in the future. We recommend adding a pre-recorded message to your phone line to explain your data policy. You should also let customers know if your calls are recorded.

What are the penalties for breaches of GDPR?

The penalty for failing to comply with the new regulation is fines of up to €20,000,000 or 4% of annual turnover in the preceding year, whichever is greater. Fines can increase if misuse of personal data continues.

What data retention policies will my funeral pre-payment plan provider set?

Funeral plan providers will have different data processes and retention policies so it is best to check directly with them. You should be aware of these processes. Your plan provider will be the data controller and you will be the data processor in relation to pre-payment plans. However, you will be the data controller for your own business.

We need to map our data processes. Is NAFD or SAIF providing a 'GDPR data processing map template' for funeral directors?

Yes, NAFD and SAIF have provided members with a sample template and some examples that you can use as a starting point. You will need to adapt these in line with your business practices and to reflect GDPR. You should do this as a priority if you have not already done so.

This document is intended to be used by funeral directing firms only. It is not intended for use by customers. This guidance is provided for information purposes and is general and educational in nature and does not constitute legal advice. It should not be considered a substitute for seeking professional help in specific circumstances. Accordingly, NAFD, SAIF, Golden Charter and Ecclesiastical Planning Services and their corporate groups shall not be liable for any losses, damages, charges or expenses, whether direct, indirect, or consequential and howsoever arising, that you suffer or incur as a result of or in connection with your use or reliance on the information provided in this guidance except for those which cannot be excluded by law. Where this guidance contains links to other sites and resources provided by third parties, these links are provided for your information only. NAFD, SAIF, Golden Charter and Ecclesiastical Planning Services are not responsible for the contents of those sites or resources. The information provided in this guidance may become out of date and may not constitute best market practice. FAQs produced April 2018.