
NAFD
GENERAL DATA
PROTECTION REGULATION
| NAFD
GDPR FREQUENTLY ASKED QUESTIONS

What is the difference between Data Controllers and Data Processors?

The Information Commissioner's Office (ICO) defines controllers and processors as:

- A controller determines the purposes and means of processing personal data. For funeral plans, this will typically be the plan provider.
- A processor processes personal data on behalf of a controller. For funeral plans, this will generally be the funeral director.
- If you are a processor, UK GDPR places specific legal obligations on you, such as maintaining records of processing activities. You are legally liable for breaches.
- If you are a controller, you remain responsible for ensuring that your contracts with processors comply with UK GDPR.
- If you offer pre-paid funeral plans, you are a data processor for your plan provider but a data controller for your own business.

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

The ICO registration fee depends on the size and turnover of your business. As fees are subject to change, visit the ICO website (www.ico.org.uk) for the most up to date information.

Who is responsible for enforcing UK GDPR?

The ICO enforces UK GDPR. Individuals can complain to the ICO if they feel their data is not being handled correctly.

How does UK GDPR affect marketing communications?

Under UK GDPR, marketing requires clear, freely given, and unambiguous consent:

- Pre-ticked boxes for consent are not valid.
- Individuals must be able to withdraw consent easily.
- Consent should be recorded, including name, date, and time.
- Funeral directors must obtain explicit consent before using data for marketing purposes.

Subject Access Requests (SARs)

- Individuals can request access to their personal data at any time.
- Businesses must respond within one month (extensions allowed for complex cases).
- Fees cannot be charged unless the request is excessive or repetitive.
- For more details, visit www.ico.org.uk.

Data Retention Policies

UK GDPR requires businesses to have a clear retention schedule for different data types. For example:

- Funeral records: Retain based on operational needs.
- Employee records: Retain according to employment law.
- Next of kin (NOK) details: Retention must be justified (e.g., for exhumation notices).
- Retention policies must be documented and made available in privacy notices.

Can funeral directors pass customer data to third parties?

Yes, but only if:

- The third party is UK GDPR compliant.
- A data processing agreement is in place.
- Data is used only for the agreed purpose and securely deleted afterward.

Can funeral directors contact families after a funeral for bereavement services?

Yes, but explicit consent is required under UK GDPR. Bereavement services, even if non-commercial, can still be considered marketing if they promote a business's brand. Consent must be:

- Freely given, specific, and informed at the time of arranging the funeral.
- Recorded properly (date, time, nature of consent).
- Withdrawable at any time, with an opt out mechanism provided.

Can funeral directors include marketing materials with invoices?

No, unless explicit consent has been obtained from the recipient beforehand. Under the Privacy and Electronic Communications Regulations (PECR) and UK GDPR, sending unsolicited marketing materials requires prior opt-in consent. An alternative approach is to:

- Ask for consent at the point of funeral arrangement.
- Offer a clear opt-in option for receiving promotional material.

Can funeral directors use old data to market to clients?

No, unless they have previously obtained valid GDPR compliant consent. If consent was not recorded or was collected before UK GDPR enforcement, it may not be valid. In this case:

- Re-consent must be obtained before using the data.
- The business should review its data retention policy to ensure old data is still necessary and relevant.

Can funeral directors share funeral attendee lists with the family?

Only if the attendees were informed about this use of their data at the time of collection. To ensure compliance:

- The funeral director should inform attendees in advance and obtain consent.
- The attendee list should not be used for any other purpose without further consent.
- Sensitive details (e.g. phone numbers, addresses) should not be shared without explicit permission.

Can Next of Kin (NoK) details be shared with charities for donation tracking?

Only with explicit consent. If donations are being forwarded to a charity, NOK details must not be shared without prior approval from the NOK. Funeral directors should:

- Include a data sharing clause in their Privacy Notice.

- Allow NOK to opt-in to share their details with charities.
- Ensure that charities handling this data are also UK GDPR compliant.

Can funeral directors pass customer data to third parties (e.g., celebrants)?

Yes, but they must:

- Ensure third parties are GDPR compliant.
- Limit data use to the specific purpose agreed (e.g. conducting a funeral service).
- Establish a Data Processing Agreement (DPA) if data processing is ongoing.
- Ensure the third party deletes personal data once no longer needed.

Are funeral directors responsible for ensuring that third parties delete data?

Yes. Under UK GDPR, data controllers must ensure that processors handle data responsibly. Funeral directors should:

- Include deletion clauses in contracts with third parties.
- Periodically review compliance with agreed data handling practices.
- Ensure third parties have proper data security measures in place.

Can client data be stored on cloud platforms (e.g., Dropbox)?

Yes, but only if the platform is UK GDPR compliant. The following steps must be taken:

- Use cloud providers with strong security measures (e.g., encryption, access controls).
- Check that data is stored within the UK or in a jurisdiction with adequate protections.
- Ensure staff are trained on how to handle data securely in cloud environments.

What happens if a family requests deletion of data that must be retained legally?

Under UK GDPR, businesses can refuse a data deletion request if they have a legal obligation to retain it. Examples include:

- Tax records (held for 7 years as per HMRC regulations).
- Contracts or service agreements.
- Records necessary for future legal claims.

However, unnecessary data should be deleted, and the business must inform the family why certain data cannot be erased.

How should funeral directors record the destruction of personal data?

A data destruction log should be maintained, including:

- What data was deleted.
- Date and method of deletion.
- Justification for deletion.
- Person responsible for deletion.

Businesses may also obtain certificates of destruction if using a third-party shredding/disposal service.

Data Security and Storage

- Businesses must implement appropriate security measures (e.g., encryption, access controls).
- Data stored online (e.g., in Dropbox) must be hosted on UK GDPR-compliant platforms.
- Data breaches must be reported to the ICO within 72 hours if they pose a risk to individuals.

Data Transfers Outside the UK

- Transfers outside the UK require adequate safeguards (e.g. Standard Contractual Clauses, adequacy decisions).
- UK-to-EU data transfers remain permitted, but additional safeguards may be needed for transfers to other countries.

Privacy and Electronic Communications Regulations (PECR)

- PECR applies to electronic marketing (e.g. emails, SMS).
- Businesses must ensure compliance with both UK GDPR and PECR.

What are the penalties for UK GDPR breaches?

Fines for non-compliance can reach £17.5 million or 4% of annual turnover, whichever is greater.

For more details, visit www.ico.org.uk.

Does UK GDPR affect funeral pre-payment plan providers?

Yes. Plan providers are data controllers, while funeral directors processing data for them are data processors. Ensure you understand your responsibilities under UK GDPR.

Data Processing Documentation

- Funeral directors should maintain a data processing map.
- A privacy notice must be available to customers (online and in business terms).
- Data breach, retention, and subject access request policies must be documented.
- Guidance documents are available from the ICO. Please visit www.ico.org.uk for more information.
- A GDPR Policy template is also included.

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.

PRODUCED BY

National Association
of Funeral Directors