Data Protection Impact Assessment (DPIA) – Burial and Cremation Team's use of a MailChimp Registration Form

---

1. Introduction

The purpose of this document is to report on and assess against any potential Privacy Impacts as a result of hosting a MailChimp registration form on the Burial and Cremation Team's SG blog page Funeral Industry News, which will serve as an initial registration portal the SG Burial and Cremation Team (the B+C Team) will utilise in its formation of a new Funeral Industry Inspectorate to plan and coordinate current and future inspections of members of the funeral industry. Members in this case include: burial authorities, cremation authorities and funeral directors.

2. Document metadata

2.1 Name of Project: Burial, Cremation, Anatomy and Death Certification Team MailChimp Registration Form

2.2 Author of report: Paul Sorensen

2.3 Date of report: 09/03/2020

2.4 Name of Information Asset Owner (IAO) of relevant business unit: Joanna Swanson

2.5 Date for review of DPIA: 09/03/2022

Review date	Details of update	Completion date	Approval Date
24/09/2020	**The EU-US Privacy Shield which Mailchimp used to safeguard transfers of personal data to its servers in the US was struck down by the European Court of Justice However, Mailchimp have incorporated Standard Contractual Clauses (SCC) into the overall contract a user signs when they opt to use the service. SCCs are currently recognised in the EEA and the UK as a safeguard for international transfers of data.**	**24/09/2020**	

	This review accounts for this change.		

3. Description of the project

3.1 Description of the work:

The Burial, Cremation, Anatomy and Death Certification Team (the B+C Team) must communicate to the funeral industry important regulatory updates and their potential impacts, including statutory inspection, as the implementation of the Burial and Cremation (Scotland) Act 2016 continues, and recently, updates in relation to the COVID-19 response. The B+C Team, thus far, has had limited success communicating with certain sections of the funeral industry, specifically, in reaching independent funeral director businesses.

The intention of the MailChimp registration form is to act as an initial registration portal for all, or as many as possible, funeral industry businesses/organisations in Scotland to sign up to. The data from which is needed to help with the future planning and coordination of inspections by the B+C Team, and to provide critical updates to industry members more generally. There are hundreds of funeral director businesses, in particular, that will soon be subject to inspection and who we do not have any, or only very limited, information on. There is a need to ensure all funeral directors are informed of regulatory changes that will directly affect them.

To direct the above to the form, the B+C Team has been working with SG marketing colleagues on a direct mail marketing campaign that will encourage funeral industry members to visit the aforementioned blog, a newly created SG Funeral Industry News page (https://blogs.gov.scot/funeral-industry/), in addition to publicly advertising key changes coming to the industry in 2020/21 and beyond. The blog and the registration form will also be promoted by the B+C Team through its existing networks.

A mock-up of the registration form is included as Annex A (design and wording of the final version may change, but not significantly. Note that we are not actively collecting any personal data, but we may incidentally collect personal data.)

We are only asking for business/organisation information, but some businesses/organisations we know from experience include peoples' first and sometimes last names as part of email addresses. E.g. Paul_Sorensen@funeraldirectorbusiness.com Or, for very small businesses, a business address may also double as the person's home address. This is what is meant by 'we may incidentally collect personal data'.

Continuing on. Once a funeral industry member registers their business/organisational details in the form, which may or may not include personal data, their information will be stored securely in the B+C Team's MailChimp account.

MailChimp is an online communication and marketing management system for sending emails, capturing subscribers' data (e.g. via forms), and storing subscribers' data in order to manage communications, etc. MailChimp facilitates General Data Protection Regulation add-ons to both their form and email template generation processes, which the B+C Team will utilise. Specifics on MailChimp's compliance with EU Data Privacy Laws and consideration of a 'hard Brexit' scenario is included further below in relevant sections.

Highlighted concerns:

Server location.
MailChimp's servers are located in the United States. (Update: 24/09/2020) However, Mailchimp have incorporated Standard Contractual Clauses (SCC) into the overall contract a user signs when they opt to use the service. SCCs are currently recognised in the EEA and the UK as a safeguard for international transfers of data.

MailChimp's Details of Data Processing outline the specifics of how they process data. The parts relevant to this exercise are outlined at the bottom of section 3.3 under MailChimp's Details of Data Processing.

MailChimp's sub-processers.
MailChimp's standard agreement that one *must* agree to before using MailChimp includes agreement that MailChimp may engage 'authorized sub-processors' to process customer data on a customer's behalf. There are 17 sub-processors at time of writing, including Google, Amazon and Zendesk. To note that Zendesk, for example, is currently used by the UK Gov's Government Digital Service (GDS) as the architecture provider for its entire internal IT support system. GDS additionally utilise MailChimp for their marking and communications needs (https://www.gov.uk/government/publications/gds-newsletter-and-event-planning-tools-privacy-notice/newsletter-and-event-planning-privacy-notice).

MailChimp does require all communications sent to customers to include a link to the MailChimp privacy policy, which outlines just how a customer's data is processed, which includes use by 'authorised sub-processors'. **By linking to this policy in all communications/forms, the B+C Team is informing people of the full use of the information they provide us. However, in addition, the B+C Team has created its own privacy policy, which is at Annex B.**

From MailChimp's Standard Terms of Use, 20. Compliance with Laws (https://MailChimp.com/legal/terms/):
"If you're located in the European Economic Area, the United Kingdom, or Switzerland (collectively, the "EEA"), and/or distribute Campaigns or other Content through the Service to, and/or otherwise collect information through the Service from, anyone located in those countries (each such Member an "EEA Member"), you agree, represent and warrant (as applicable) to MailChimp that:
You will clearly post, maintain, and abide by a publicly accessible privacy notice on the digital properties from which the underlying data is collected that (a) satisfies the requirements of applicable data protection laws, (b) describes your use of the Service, and (c) includes a link to MailChimp's Privacy Policy."

3.2 Personal data to be processed:

Variable	Data Source
POSSIBLE – first name	Funeral industry members who are interested in subscribing and receiving updates on the regulation of the funeral industry direct from The Scottish Government, in part to prepare for upcoming inspections, *may* have a business/organisation email address that contains their first name.
POSSIBLE – last name	Same as above.
POSSIBLE – home address	Same as above, but address. It is unlikely that the B+C Team would know if the address is also a home address until that location was inspected. There will be a specific question asking the subscriber to select if this is also a home address.

3.3 Describe how this data will be processed.

The MailChimp registration form will be hosted as a link to a pop-up form on the blog. The B+C Team's MailChimp account stores the data collected in the form in the B+C Team's MailChimp account and sends a notification of a new registration to the BurialandCremation@gov.scot mailbox, a restricted mailbox (assessable by the B+C Team only).

The MailChimp account itself is only accessible by the B+C Team. Additionally, data may be input from MailChimp by the B+C Team into spreadsheet/s hosted in a restricted file in an internal Scottish Government filing system called eRDM (again, the section where a spreadsheet may be saved is accessible only by the B+C Team), as a backup to mitigate the risk of a loss of data or loss of MailChimp account access and utilised for communicating information and updates relevant to the funeral industry, as well as assisting in the future planning and coordinating of inspections. No other use of this data will occur.

The form will include the following data use permission statement:

The Scottish Government is working to provide relevant and direct information to burial authorities, cremation authorities, funeral director businesses and other interested parties, with regards to the implementation of the Burial and Cremation (Scotland) Act 2016 and its related regulations, as well as on other relevant information for Scotland's funeral industry. The Scottish Government will also use the data collected in this form to plan and coordinate current and future inspections of the funeral industry. This form allows you to register your business/organisation details, so they can be used by The Scottish Government for the purposes stated. By ticking the 'I consent to my data being used in this way' box, you agree to the stated conditions of use.

Additionally, the aforementioned MailChimp privacy policy statement sits above the 'register' button on the form (again, see Annex A).

Before being able to click the 'Register' button on the form, the subscriber must agree to the conditions of data use.

Subscriber's data will be held for an initial two years and will be reviewed by the Burial and Cremation Team (Update 24/09/2020 – reviewed on this date) at this point for further retention (coinciding with the review of this document). Data collected and processed will not be held or further used unless it is essential to communicate to members of the funeral industry important regulatory updates and their potential impacts, including statutory inspection, or to plan and coordinate current and future inspections of the funeral industry, (Update 24/09/2020 or to continue to provide information relevant to the industry on COVID-19).

All data will be gathered directly from the subscriber submitting the form.

MailChimp account security and privacy policy

MailChimp's security includes keeping account information hashed, which means they are not able to see a Member's (the B+C Team) account information beyond basic information. For example, they cannot resend forgotten passwords. They will only provide Members with instructions on how to reset them. (https://MailChimp.com/legal/privacy/#5._General_Information)

MailChimp's security practices cover: data centre security, protection from data loss/corruption, application level security, internal IT security, internal protocol and education, credit card processing security, security against compromised accounts in case of hacking, as well as a section on how they continue to invest in privacy/security (e.g. they retain a law firm in the UK to consult on EU privacy issues): https://MailChimp.com/about/security/

Some MailChimp employees necessarily have access to Member's account's data, including customer data (such as MailChimp's tech support and their engineers). Under the Internal Protocol and Education section of the above linked security information page, MailChimp mitigates the risk of employee data misuse by having all people who work in teams that have access to customer data undergo criminal history and credit background checks prior to employment, as well as sign a Privacy Safeguard Agreement outlining the individual's responsibility in protecting customer data.

MailChimp data is kept in data centres in separate databases that are kept separate and dedicated to preventing corruption and overlap. MailChimp has something they refer to as 'multiple layers of logic', which segregates user accounts from each other. Data centres are physically secured 24/7 and include biometric scanners for staff members. DDOS mitigation is also in place at all data centres.

MailChimp's Details of Data Processing (relevant parts)
(https://MailChimp.com/legal/data-processing-addendum/#Annex_A_%E2%80%93_Details_of_Data_Processing).
International Transfers.
Data centre locations (some of this has been touched on above in 3.1). The Customer (the B+C Team) acknowledges that MailChimp may transfer and process Customer Data to and in the United States and anywhere else in the world where MailChimp, its Affiliates or its Sub-processors maintain data processing operations. MailChimp shall at all times ensure that such transfers are made in compliance with the requirements of EU Data Protection Laws.

European Data transfers specifically.
To the extent that MailChimp is a recipient of Customer Data protected by EU Data Protection Laws ("EU Data"), the parties agree that MailChimp makes available the mechanism listed below:

Standard Contractual Clauses (SCCs): MailChimp agrees to abide by and process EU Data in compliance with the SCCs, which are incorporated in full by reference and form an integral part of this DPA. For the purposes of the SCCs: (i) MailChimp agrees that it is the "data importer" and Customer is the "data exporter" under the SCCs (notwithstanding that Customer may itself be an entity located outside the EU); The parties further agree that the SCCs will apply to Customer Data that is transferred via the Service from Europe to outside Europe, either directly or via onward transfer, to any country or recipient: not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Law).

Return or Deletion of Data
Duration of processing: MailChimp will process Customer Data as follows: Deletion on termination. Upon termination or expiration of the Agreement, MailChimp shall (at Customer's election) delete or return to Customer all Customer Data (including copies) (in this case to the Scottish Government) in its possession or control, except that this requirement shall not apply to the extent MailChimp is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data MailChimp shall securely isolate, protect from any further processing and eventually delete in accordance with MailChimp's deletion policies, except to the extent required by applicable law.

3.4 Explain the legal basis for the sharing with internal or external partners.

Data will be shared to external partners by the B+C Team. Data will be shared with inspectors, who are by Ministerial appointment and are Data Controllers in their own right. The basis for gathering the data falls under the B+C Team's remit as the SG policy developer in respect to the regulation of the funeral industry and the B+C Team's need to communicate developments to this industry and to inspect this industry. The sharing of data with inspectors is required to fulfil the inspection function.

Public Task is the legal basis of this initiative. The gathering of this data is necessary to communicate key information to the funeral industry that will affect the funeral industry, and is necessary to plan and coordinate current and future inspections. Data will not be retained for any other purpose and data will never be collected without the consent of the individual.

The B+C Team has, via the settings in its MailChimp account, turned off all possible data sharing settings. E.g. MailChimp's data analytics settings. The B+C has, additionally, 'turned off' predicted demographics in its MailChimp account, which states it pulls information from customers to enhance the marketing aspect of the Mailchimp service. See below:

Data analytics setting [In MailChimp Account Options]

"Some MailChimp features, like product recommendations and predicted demographics, analyse information from user accounts to provide dad-driven predictions and recommendations. This data includes personal information about contacts. We also use account data to build and improve our products and services.

Your participation improves these features and helps all users achieve their marketing goals. MailChimp takes data privacy seriously. For more information about how we treat your data, visit our Privacy Policy.

Select your data usage preferences with the following settings.

[unticked box] Include my data in MailChimp's data analytics projects.

[unticked box] Turn on predicted demographics in this account.
Predicted demographics data is available for MailChimp Pro, or paid accounts with a connected store."

Finally, we have not authorised any connections with partners of MailChimp, e.g. Facebook, Twitter, Google Analytics, etc.

4. Stakeholder analysis and consultation

4.1 List all the groups involved in the project, and state their interest.

Group	Interest
Scottish Government Burial, Cremation, Anatomy and Death Certification team, Health Protection Division.	Gathering business/organisation contact and registration information, which may incidentally include personal information, from funeral industry members to deliver direct updates on regulations and other relevant topics, as well as to compile a funeral industry database in order to plan and coordinate current and future inspections.
Joanna Swanson, Deputy Director, Health Protection Division	IAO/Head of the division in which the B+C Team is sited.
Inspectors of Burial, Cremation and Funeral Directors	Ministerial appointees and Data Controllers in their own right, inspectors work closely with the B+C Team in respect to both communicating with industry and undertaking inspections.
MailChimp	The third-party service provider used to facilitate the above. The data processor.

Funeral industry members	Burial and cremation authorities and funeral director businesses. The subscribers.

4.2 Method used to consult with these groups when making the DPIA.

Funeral industry members were made aware of a new registration form feature to be added to the blog in an email that was sent to stakeholders through the Notify email system with the subject line: Coronavirus guidance for funeral directors, a new blog, and an up-coming funeral industry registration process. The body of the email revealed that we will soon have a registration form up and running, hosted on the blog, for all of Scotland's funeral industry members to register some basic details with us, such as their company name and address, as part of an initial registration exercise.

4.3 Method used to communicate the outcomes of the DPIA.

Blog post pointing to the DPIA once published to the SG website.

5. Questions to identify privacy issues

5.1 Involvement of multiple organisations

MailChimp

5.2 Anonymity and pseudonymity

There will be no combination of data from multiple systems. No new or future dataset will be produced from the data gathered. No personal information will be intentionally requested.

5.3 Technology

Registration form hosted by MailChimp, the Burial and Cremation Team's SG mailbox and protected eRDM file (for record keeping/backup contingency).

5.4 Identification methods

The registration form asks for business/organisation name, address and contact information, however, subscribers may have email addresses with personal names as part of a business email address and/or their business address is also a home address.

5.5 Sensitive/Special Category personal data

No personal information such as bio-metric, bank account, NIN numbers, etc. or any special category or sensitive personal data will be gathered.

5.6 Changes to data handling procedures

Data will be captured by a MailChimp hosted form, which will store the data and notify the B+C Team's mailbox in an 'activity summary' email sent at the end of each day. The data will additionally be stored in a spreadsheet(s) in eRDM in a file restricted to the B+C Team for the purposes of having a record of funeral industry members/contingency backup. Access to the SG mailbox is also restricted to members of the B+C Team.

Risk assessment requirements will be factored into any changes to data handling procedures, in particular Risk 03 (see below for specifics).

5.7 Statutory exemptions/protection

N/A

5.8 Justification

Again, relates to Public Task. We need to compile a comprehensive list of funeral industry members for the purposes of communicating key information to industry without having to rely on third party organisations, and, chiefly, to be able to plan and coordinate current and future inspections of the industry. We will encourage all industry persons to sign-up and be engaged with the B+C Team via our direct marketing campaign and existing network channels. All of the funeral industry will soon be subject to statutory inspections, the B+C Team, therefore, needs to know business details of every industry member.

5.9 Other risks

Specific risks are highlighted in Section 7, below.

6. General Data Protection Regulation (GDPR) Principles

Principle	Compliant – Yes/No	Description of how you have complied
6.1 Principle 1 – fair and lawful, and meeting the conditions for processing	Yes	**Lawfulness** We have identified an appropriate lawful basis (or bases) for our processing. Public Task: Article 6(1)(e) gives you a lawful basis for processing where: "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" We don't do anything generally unlawful with personal data. **Fairness** We have considered how the processing may affect the individuals concerned and can justify any adverse impact. We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified. We do not deceive or mislead people when we collect their personal data. People registering are informed as to what they are registering for, as well as being notified of MailChimp's privacy policy. **Transparency** We are open and honest, and comply with the transparency obligations of the right to be informed. We have created our own privacy policy, which is at Annex B.

		Data will be available to the 4 people in the B+C Team, Joanna Swanson as Deputy Director and IAO, the inspectors, and MailChimp as data processor. Data will be collected into the B+C Team's MailChimp account, which is assessable only by the B+C Team. Data will also be stored in a restricted (to the B+C Team + Joanna Swanson) file on eRDM in a spreadsheet(s). Data stored will be subject to review in 2 years' time as to whether or not it is retained or securely deleted. If it is no longer being used, it will be deleted. MailChimp allows secure data deletion, as detailed above.
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.2 Principle 2 – purpose limitation	Yes	We have clearly identified our purpose or purposes for processing. We have documented those purposes. We include details of our purposes in our privacy information for individuals. We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals.
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.3 Principle 3 – adequacy, relevance and data minimisation	Yes	Similar to the purpose limitation section above, we are collecting data required to send industry communications and to inform a register. Registration is voluntary and self-removal from MailChimp is simple – built into the MailChimp system, a user can easily unsubscribe from further messages via a 'single click' mechanism, which stems from their GDPR compliance additions. Again, data deletion is also possible. We are only collecting personal data we actually need for our specified purposes. We have sufficient personal data to properly fulfil those purposes. We periodically review the data we hold, and delete anything we don't need.

Principle	Compliant – Yes/No	Description of how you have complied
6.4 Principle 4 – accurate, kept up to date, deletion	Yes	Data is generated and provided solely by the subscribers. Data will only be updated or modified if a subscriber resends the registration form, or contacts us to change any details. We ensure the accuracy of any personal data we create. We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data. We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary. If we need to keep a record of a mistake, we clearly identify it as a mistake. We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data. As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data.
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.5 Principle 5 – kept for no longer than necessary, anonymization	Yes	Subscribers will be able to request, via MailChimp, which is fully GDPR compliant, to 'opt-out' of any further communications from the B+C Team after registration. We will get a notification of this and will additionally delete that business/organisation's data securely from our eRDM backup record (a spreadsheet/s). No subscriber in the course of receiving communications from us will be able to see any other subscriber's information. Messages will be sent *en masse*, but akin to sending an email to a group of people as blind carbon copied, which is how MailChimp functions. There is no mechanism to accidently include other subscriber's information as part of a mass communication.
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.6 GDPR Articles 12-22 – subscriber rights	Yes	The GDPR provides the following rights for individuals: Public Task as detailed in Privacy Notice: 1. The right to be informed 2. The right of access

		3. The right to rectification 4. The right to restrict processing 5. The right to object 6. Rights in relation to automated decision making and profiling.
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.7 Principle 6 - security	Yes	We have considered and put in place the following: 'Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk'.
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.8 GDPR Article 24 - Personal data shall not be transferred to a country or territory outside the European Economic Area.	Yes	Mailchimp have incorporated Standard Contractual Clauses (SCC) into the overall contract a user signs when they opt to use the service. SCCs are currently recognised in the EEA and the UK as a safeguard for international transfers of data.

7. Risks identified and appropriate solutions or mitigation actions proposed

Is the risk eliminated, reduced or accepted?

Risk	Ref	Solution or mitigation	Result
Risk of loss of data at any point	01	Accepted risk that in all digital data transfer there exists a risk to loss of data. SG Cyber Security and Defence has been consulted on this subject. They have confirmed there are no formal procedures for using MailChimp within the SG. However, they confirm that there are departments within SG who use MailChimp. Their advice is that if the initiative includes gathering of any form of sensitive information then MailChimp should not be used (we are not requesting any sensitive information and MailChimp's own position on sensitive data processing is: [under Annex A of MailChimp's 'Details of Data Processing' *"(g) Sensitive Data: MailChimp does not want to, nor does it intentionally, collect or process any Sensitive Data in connection with the provision of the Service."* (https://MailChimp.com/legal/data-processing-addendum/#Annex_A_%E2%80%93_Details_of_Data_Processing). SG Cyber Security and Defence has made us aware that it has been known for recipients of these mail campaigns to also be added to spam lists as their information is often farmed from MailChimp itself. This is tied into MailChimp's privacy policy. Subscribers are required in all communications and the form to be	Accept

		directed to the MailChimp privacy policy. The B+C Team has reduced the chance of data being farmed by 'opting out' of as many data sharing features as permitted. Further, the data the B+C team is requesting is not personal information, we only may incidentally receive it, which further lowers the risk of any data farming/breach.	
Risk of MailChimp server failure leading loss of access to data temporarily	02	Accepted risk that such an event may occur. MailChimp is one of the World's largest companies in the field of online communication/marketing, however. This impact is further mitigated by the B+C Team's duplication of the data received in eRDM.	Accept
Risk of transferring personal data out of the EEA	03	Low risk as there is no transfer of special category or sensitive data. The European Commission has the power to determine, on the basis of article 45 of Regulation (EU) 2016/679 whether a country outside the EU offers an adequate level of data protection. The adoption of an adequacy decision involves: • a proposal from the European Commission • an opinion of the European Data Protection Board • an approval from representatives of EU countries • the adoption of the decision by the European Commission. At any time, the European Parliament and the Council may request the European Commission to maintain, amend or withdraw the adequacy decision on the grounds that its act exceeds the implementing powers provided for in the regulation. The effect of such a decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary. In others words, transfers to the country in question will be assimilated to intra-EU transmissions of data. Mailchimp have incorporated Standard Contractual Clauses (SCC) into the overall contract a user signs when they opt to use the service. SCCs are currently recognised in the EEA and the UK as a safeguard for international transfers of data.	Accept

8. Incorporating Privacy Risks into planning

Explain how the risks and solutions or mitigation actions will be incorporated into the project/business plan, and how they will be monitored. There must be a named official responsible for addressing and monitoring each risk.

Risk	Ref	How risk will be incorporated into planning	Owner
Risk of loss of data at any point	01	We'll have early sight of any data loss if forms appear empty or missing information. However, we will	Paul Sorensen

		extensively test the use of the form before it goes 'live'.	
Risk of MailChimp server failure leading loss of access to data temporarily	02	Accepted risk that such an event may occur. MailChimp is one of the World's largest companies in the field of online communication/marketing, however. This impact is further mitigated by the B+C Team's duplication of the data received in eRDM.	Paul Sorensen
Risk of the United States of America's or MailChimp's status change in respect to the adequacy decision and Privacy Shield Framework	03	The B+C Team will commit to regularly checking the status of both the United States of America in respect to the EC adequacy decision and MailChimp as an 'Active Participant' of the Privacy Shield Framework. (Update: the EU-US Privacy Shield which Mailchimp used to safeguard transfers of personal data to its servers in the US was struck down by the European Court of Justice However, Mailchimp have incorporated Standard Contractual Clauses (SCC) into the overall contract a user signs when they opt to use the service. SCCs are currently recognised in the EEA and the UK as a safeguard for international transfers of data. This review of 24/09/2020 accounts for this change.)	Paul Sorensen

9. Data Protection Officer (DPO)

The DPO may give additional advice, please indicate how this has been actioned.

Advice from DPO	Action

10. Authorisation and publication

The DPIA report should be signed by your Information Asset Owner (IAO). The IAO will be the Deputy Director or Head of Division.

Before signing the DPIA report, an IAO should ensure that she/he is satisfied that the impact assessment is robust, has addressed all the relevant issues and that appropriate actions have been taken.

By signing the DPIA report, the IAO is confirming that the impact of applying the policy has been sufficiently assessed against the individuals' right to privacy.

The results of the impact assessment must be published in the eRDM with the phrase "DPIA report" and the name of the project or initiative in the title.

Details of any relevant information asset must be added to the Information Asset Register, with a note that a DPIA has been conducted.

I confirm that the impact of undertaking the project has been sufficiently assessed against the needs of the privacy duty:

Name and job title of a IAO or equivalent	**Date each version authorised**
Elizabeth Sadler, Deputy Director, Health Protection Division	Version 1: 24/03/2020
Joanna Swanson, Deputy Director, Health Protection Division	Version 2: 24/09/2020

Annex A – The registration form. Subject to change (no change to personal data collected, however)

Business/Organisation Email Address

Business/Organisation Name

Business/Organisation Address
Address Line 2
City
State/Province/Region
Postal/Zip Code
Country: United Kingdom [default]

Business/Organisation Phone Number

Affiliation [No affiliation; Burial authority; Cremation authority; Funeral director; Other]

Data Use Permission
The Scottish Government is working to provide relevant and direct information to burial authorities, cremation authorities, funeral director businesses and other interested parties, with regards to the implementation of the Burial and Cremation (Scotland) Act 2016 and its related regulations, as well as on other relevant information for Scotland's funeral industry. The Scottish Government will also use the data collected in this form to plan and coordinate current and future inspections of the funeral industry. This form allows you to register your business/organisation details, so they can be use by The Scottish Government for the purposes stated. By ticking the 'I consent to my data being used in this way' box, you agree to the stated conditions of use.

I consent to my data being used in this way.

You can unsubscribe at any time by clicking the link in the footer of our emails. For information about our privacy practices, please visit our blog page: Funeral Industry News.

Annex B – The Burial and Cremation Team's Privacy Notice

Burial and Cremation Team, Scottish Government Privacy Notice

Our contact details

Postal address:
Burial and Cremation Team (3E)
Health Protection Division
The Scottish Government
St. Andrew's House
Edinburgh
EH1 3DG

Email address: burialandcremation@gov.scot
Phone number: 0300 244 4000 (08:30-17:00, M-F)
Blog: https://blogs.gov.scot/funeral-industry/
Main contact person: Paul Sorensen

What type of information we have

We (The Burial and Cremation Team) do not intend to collect personal data. However, if you register your business information with us via our MailChimp hosted form on our blog, you may incidentally supply us with personal data in the form of your first and/ or last name if it forms part of your business email address. Additionally, you may incidentally supply us with personal data in the form of your home address if this address also serves as your business address.

How we get the information and why we do we have it

We will receive your business information, which may contain the personal data noted above, from you directly, once you have submitted it via our MailChimp hosted form on our blog.
The reason we require your business information is two-fold. Firstly, we need to be able to directly communicate changes in laws and regulations to you as a member of Scotland's funeral industry. The changes affect you and you need to be given the right information at the right time to begin to prepare, or to be aware of, upcoming changes, some of which will be statutory requirements.

Secondly, we require your business information in order to plan and arrange inspections of your business, under the Burial and Cremation (Scotland) Act 2016.
The lawful basis for collecting your business information, which may contain the personal data noted above, is Public Task.

Public Task - The gathering of this data is necessary to communicate key information to the funeral industry that will affect the funeral industry, and is necessary to plan and coordinate current and future inspections. Data will not be retained for any other purpose and data will never be collected without the consent of the individual.
At this stage, the business information we require is being collected on a voluntary basis. It is likely in the future that you will be required to submit your business information, as well as other information, such as personal information. The details of this expanded collection of data has yet to be specified.

What we do with the information

We will use your business information to contact you through MailChimp when there is information relevant to you as a member of the funeral industry. Most communications will be around preparedness for an upcoming inspection regime we are developing for the funeral industry across Scotland. We may also communicate blog updates to you from time to time. All communications will always be relevant to you as a member of the funeral industry operating in Scotland.

MailChimp, who hosts our form, stores your information. We have 'opted-out' of all information sharing agreements via our MailChimp account. However, it is possible that some information is still shared by MailChimp to their selected partners who may be located outside of the European Economic Area (EEA).

However, the European Commission has determined that the United States of America and MailChimp (as an 'Active Participant' of the Privacy Shield Framework) offers an adequate level of data protection to handle EU data. The Burial and Cremation Team has committed to regularly checking this status as it is subject to change with no notice given. We will contact you should the details of this arrangement change and inform you of our response at that time, if required.

How we store your information

When you submit your business information to us via our MailChimp hosted form on our blog, all that information is stored in our MailChimp account. Additionally, as a back-up, we will duplicate your information on our own Scottish Government secured filing system. Only our Burial and Cremation Team will have access to your information. Information stored by the Scottish Government is subject to our standard information processing procedures.

We plan to keep your information for an initial two years from the date you submit it. At which point we will review our use of it. If we are still using it to, for example, contact you or to plan inspections, we will keep it and set another review date. If we are not still using your information for those stated purposes, we will schedule it for secure deletion as per Scottish Government standard information processing procedures.

You can, at any time, request not to receive communications from us, or request to have all information we hold on you to be securely deleted. You can do this via a link provided in any of our MailChimp emails, or via a request to burialandcremation@gov.scot

Your data protection rights

You have the right to request access to the personal data that we hold about you.

You have the right to object to the processing of your personal data.

Under the lawful basis of Public task, the processing of your business information is necessary for us to perform a task in the public interest, or for our official functions, and the task or function has a clear basis in law (in our case the Burial and Cremation (Scotland) Act 2016 and its regulations).

If you are unhappy with the way in which we have processed your personal data then you have the right to complain to a supervisory authority (such as the Information Commissioner's Office (ICO) Scotland).

How to complain

If you wish to exercise any of these rights, please contact burialandcremation@gov.scot or contact the ICO Scotland:

The Information Commissioner's Office - Scotland
45 Melville Street
Edinburgh
EH3 7HL

Telephone: 0303 123 1115

Email: Scotland@ico.org.uk