



Guidance on the Arts Council's Data Protection Compliance

Document Ownership: Data Protection

Version Control: Version 1.0

Contents

Guidance on the Arts Council’s Data Protection Compliance 1

Document One: Data Processing Agreement 3

Document Two: Third Party Data Protection Assessment (Longform) 6

 Instructions for Longform Third Party Data Protection Assessment..... 6

Document Three: Data Protection and Information Security Third Party Assessment (Microform) ... 9

 Instructions for Micro Data Protection and Information Security Assessment 10

Guidance for Third Parties on Arts Council Data Protection Compliance Requirements

Document One: Data Processing Agreement

The Arts Council has data protection obligations under the General Data Protection Regulation ('GDPR'). One of these obligations is called a Data Processing Agreement (DPA).

DPAs are required under the GDPR where data is transferred between parties, they are legally binding and are to be signed between the Data Controller (the Arts Council) and the Data Processor (third party).

The Data Protection Commission, the Irish data protection authority, has provided some guidance around Controller and Processor arrangements that you can view at [Controller and Processor relationships | Data Protection Commission](#).

What do I need to complete?

Page 1: Include your / your organisation's name and address.

Page 10: Include your name, job title, signature and the date. This signature can be completed digitally as long as you are sending the DPA back from your professional / named email address.

Page 11: Please complete Appendix A in full.

This section is to be completed by the external party (not the Arts Council). We ask that you read the agreement and complete Appendix A, ensuring all sub-processors (e.g., third parties you use such as Microsoft, Stripe etc.) are listed in the table. Please indicate if any processing is undertaken outside the EEA and if so, what mechanism is in place with that processor to transfer the data (Standard Contractual Clauses, Adequacy Decisions, etc). If you are not sure, please contact our Data Protection team for assistance.

Data processing agreements need to include the purpose and scope of processing data, what kind of data will be processed, how it can be protected, and establishing the relationship between the controller and processor of such data – and this section is where to do so.

Please see below explanation on what needs to be completed on this page:

- 1.1 **Subject matter of processing**: This is a description of the general objective or task.
- 1.2 **Nature of processing**: This is how you will carry out the general objective or task.
- 1.3 **Purpose of processing**: This is the purposes for which you will be carrying out work for the Arts Council e.g., to send marketing communications, to provide assessment services for funding applications etc.
- 1.4 **Duration of the processing**: This is usually the length of the contract.
- 1.5 **Types of personal data**: This will be what data you will be processing e.g., names, email addresses, addresses, artist CVs, application forms. This is anything that can be used to

identify an individual that you will use, store, access and so on during your engagement with us.

1.6 Categories of data subject: This is the kind of individual the data you will be dealing with in your work for the Arts Council e.g., artists, employees, organisations, funding applicants etc.

1.7 List of Sub-processors to be completed by the Data Processor in table.

This is a list of any other parties/software etc that you will be using for operations on Arts Council data. Please complete this table fully with any other parties listed. This should mirror parties you list in the Data Protection Questionnaire.

Table

Sub-processor Name: This is the name of the other party/software. Some common parties include Microsoft, Adobe, SurveyMonkey etc.

Purpose for Processing: This is the purpose or reason that you use the other party / software. For example, to send surveys, for email communications etc.

Data Processed: This is the Arts Council data that will be processed by the party / software e.g., Name, contact information, financial information, employment information etc.

Sub-processor location: This is where Arts Council data will be geographically stored by the party / software. You will need to get Arts Council approval if this is outside of the EEA/EU. For example, Microsoft allows EU businesses to have their data stored in the EU and usually has two data storage locations e.g., Ireland and the Netherlands. To find this out you can contact the party, visit their website and view their Privacy Notice, or look at the contract you have with them.

Mechanism relied on: This is where the data is being transferred outside of the EU/EEA. Under the GDPR data can only be transferred outside of the EU/EEA where there is an equivalent protection of data or safeguards in place.

There is a list of countries that have been deemed to provide an equivalent protection of data as the EU/EEA. These countries are seen to be adequate for data transfers:

Andorra, Argentina, Brazil (mutual adequacy decision with the EU), Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, South Korea, Switzerland, United Kingdom, Uruguay.

A note on the United States

If a party is listed on what is called the EU-US Data Privacy Framework, then they have been assessed and deemed to provide adequate protection of data. You can view the list at this [website](#). If a company is not on this list, you will need to discuss this with the Arts Council Data Protection team.

If data is being processed by a party that is not listed above, you will need to speak to the

Arts Council Data Protection team.

General FAQs around the Data Processing Agreement

What do you mean by controller and processor?

All definitions are included within the DPA, under Section 1 'Definitions and Interpretations'.

Why are the Arts Council implementing updated data protection terms?

To...

- Ensure compliance with data protection laws;
- Protect the rights of individuals;
- Safeguard the confidentiality of personal data;
- Minimise the risks including unauthorised access to personal data;
- Establish an accountability framework for the handling of personal data.

Do I/we need to sign this agreement?

The ultimate purpose of a data processing agreement is to guarantee that there will be sufficient data protection guarantees between parties.

The Arts Council is required to have such agreements in place with parties that process personal data on our behalf. We have a responsibility to ensure compliance with data protection laws. If you do not wish to sign this agreement, the Arts Council may not be able to continue our engagement with you.

Are there particular sections I/we should pay attention to?

Yes, there are some new terms around...

- Data breaches e.g., responsibilities where there is a breach (such as a cyber incident);
- Data subject requests e.g., responsibilities where an individual who makes a request around their personal data as required under the GDPR;
- Technical and Organisational measures e.g., security measures ('TOMS'); and
- Requirements to support the Arts Council in conducting a Data Protection Impact Assessments.

Who can I/we contact if we have questions about this agreement?

You can contact the Arts Council's Data Protection by emailing dataprotection@artscouncil.ie.

Document Two: Third Party Data Protection Assessment (Longform)

You will either be asked to complete one of the following two assessment forms (longform or microform). The longform is the default form, if you wish to complete the microform you can apply to use this by emailing your Contract Manager in the Arts Council.

The longform is intended to assess your ability to meet data protection requirements where you will process Arts Council personal data. Where we have asked you to complete the longform, this will be due to the size of your organisation and/or the scale or risks around data processing.

What are we looking for?

- Be accurate and transparent in your response.
- Ensure that you have up to date Anti-Virus/Anti-Malware End Point Protection.
- Overall level of data protection awareness and compliance measures in place.
- No excessive collection or retention of Arts Council data.
- Sufficient measures in place to ensure the confidentiality and integrity of Arts Council data.
- No Arts Council Data is to be exposed to AI Agents.
- All cloud hosted services are secure, with data stored within EEA and have MFA enabled.
- Data transfers to non-EU countries have a mechanism for which to do so and appropriate assessments have been carried out.
- There is no sharing of Arts Council data that the Arts Council is not aware of, and where there is data sharing it is done securely and confidentially.
- Separated Work and personal spaces e.g. iCloud segregated.

Instructions for Longform Third Party Data Protection Assessment

Please ensure to complete the table on page 2 with details of the engagement e.g., your name, contact details etc.

Supplier Due Diligence Questions

What is the nature of the data you will be processing? (Editable list including Personal data Special Category Data, Data relating to criminal offences and convictions, no personal data being processed)

Please select the relevant type of data you will be processing (e.g., using, storing etc) on behalf of the Arts Council. You do not need to provide details of what the data is here, only select the relevant choice from the list (e.g., personal data).

- Personal Data: This includes any data that can be used to identify an individual e.g., names, email addresses etc).
- Special Category Data: This is more sensitive personal data and includes data listed in the box below such as health data).
- Data relating to criminal offences and convictions: This is where you would be processing data about criminal convictions.
- No personal data: This is where there is no data being processed that can identify an individual. For example, if you are working with survey results that are anonymous.

What categories of personal data are being processed? (Editable list).

Please select the relevant type of data you will be processing (e.g., using, storing etc) on behalf of the Arts Council. You do not need to provide details of what the data is here, only select the relevant choice/s from the list.

- Identification Data (e.g., names, ID cards, passports).
- Contact Data (e.g., email address, phone numbers).
- Communications Data (e.g., email communications, text messages).
- Web Data (e.g., website views, web forms).
- Log Data (e.g., back up logs).
- Physical characteristics Data (e.g., data relating to health and other physical characteristics).
- Finance and Tax Data (e.g., bank and financial statements, PPSN, funding histories).
- HR Data (e.g., CVs, contracts, other records of employment).
- Performance Data (e.g., records of employee performance).
- Location Data (e.g., IP addresses, Eircode).
- Social and Marketing Data (e.g., social media handles, records relating to marketing campaigns).
- Photography and Video Content (e.g., recordings of events, images of individuals).
- CCTV Data (e.g., CCTV footage).
- Voice Recording Data (e.g., an application being utilised where an individual's voice is recorded, video recordings where individuals' voices are being recorded).
- Other [Please list] (e.g., any other type of data not listed above).

What Special Categories of Personal Data are processed? (Editable list).

Please select the relevant type of special category data you will be processing (e.g., using, storing etc) on behalf of the Arts Council. This is personal data that is considered more sensitive in nature. You do not need to provide details of what the data is here, only select the relevant choice/s from the list.

- Health information (e.g., medical certificates and health records).
- Political opinions (e.g., information that provides for an individual's political opinions).
- Race, Ethnic Origin (e.g., nationality listed on documentation).

- Biometric Data (e.g., fingerprints, retinal scans)
- Membership or activity in a trade union (e.g., union registration number).
- Sexual Orientation, Sexual Preferences (e.g., records that identify an individual's sexual orientation or sex life).
- Religious or philosophical beliefs (e.g., dietary requirements can infer religion).
- No Special Category Data (e.g., where there is none of the above).

Please confirm the location(s) where personal data will be processed by the Supplier (where are you accessing the data from e.g., London office) and please confirm the location(s) where personal data will be stored/hosted (e.g., Amazon Europe Frankfurt and Dublin)

Please include all locations that data will be processed (e.g., accessed, stored etc). This will include physical and digital storage as an example: physical files in office, cloud back-ups in Microsoft data centres in Frankfurt and Dublin, Adobe cloud in Ireland etc. Please provide as much information here as you can. For more on Data Locations please see information under the Data Processing Agreement instructions above.

Has the Supplier received any data protection related fines or sanctions, or any other regulatory fines or sanctions, or is it currently subject to any statutory investigation by any Supervisory Authority or any other governing body or state agency? If yes, please provide details.

Please include any fines or reprimands your organisation have had (for example under the General Data Protection Regulation) as well as any investigations (e.g., Central Bank, Revenue etc) you have been or are currently subject to.

Supplier Organisational Measures

This section requires you to provide assurances around your compliance with relevant data protection laws and your practices.

Data Protection Policies and Procedures

If you do not have the documentation or processes in place, do not tick the box. If you have some of the facets listed but not all, please just note the elements you do have.

Policy Review

Please tick the box if data protection policies are reviewed on an annual basis and approved by management. If you do not do this, please leave it blank. If you review at different intervals, please note this in the comment box.

Appointment of a Data Protection Officer/Data Protection Lead

Where you have a responsible person for data protection in place please tick the box. If you do not have a responsible person for data protection do not tick the box. If you do not have a responsible person for data protection, please just note this in the comments box. Please note

there are certain circumstances where having a Data Protection Officer is mandatory under the General Data Protection Regulation.

Supplier Staff (including Contractors)

Where you have staff and/or contractors in place please tick the boxes as relevant for the measures you have in place. If you do not have measures do not tick the boxes. If you do not have staff and/or contractors in place, please just note this in the comments box as N/A.

Data Transfer Management

Please confirm if due diligence, e.g., checking that suppliers have appropriate data protection practices is carried out and that you have compliant Data Processing Agreements are in place (DPAs including data breach responses, data subject requests etc). If you do not do this, please leave blank.

International Transfers

Please confirm if you carry out Transfer Impact Assessments where there is international e.g., outside of EEA/EU transfers occurring. Further information on transfers can be found under Section 1 Data Processing Agreement, under 1.7. If you do not carry out Transfer Impact Assessments, please leave this blank.

Breach Management Policy

If you have policies and procedures relevant to personal data breach management in place and maintained please tick this box, if not leave it blank.

Data Subject Rights Request (DSR) Management

Please tick the box if you have appropriate policies and procedures for Data Subject Rights Management in place. Data Subject Rights under the GDPR are where individuals have rights to access, deletion etc. in relation to their own personal data. For more information, please see the Data Protection Commission [website](#).

Supplier Technical Measures

Please note that responses to this section are cumulative.

Data Retention and Deletion

Please tick this box if you have a Retention Policy in place, retention and data management policies, you purge Arts Council data or intend to, and that you carry out regular data audits (e.g., to ensure that retention periods are being followed. If you do not, please do not tick the box.

Secure Storage and Transfer of Data (Data Handling)

Please tick this box if you have appropriate security measures in place as described. If not, please leave blank.

Remote Working

If you have remote workers (e.g., workers outside of your jurisdiction/office) please tick this box if you have the measures in place as described. If not, please leave blank.

Data Retention and Deletion (Solutions)

This question is for solution providers only (e.g., if you are providing software). Please tick the box if the solution has retention configurations.

Who can I/we contact if we have questions about this assessment?

You can contact the Arts Council's Data Protection team by emailing dataprotection@artscouncil.ie.

Document Three: Data Protection and Information Security Third Party Assessment (Microform)

This form is intended as a more proportionate version for individuals, sole traders and microbusinesses, combining key data protection and information security questions in a lighter format.

The microform is intended to assess your ability to meet data protection requirements where you will process Arts Council personal data. Where we have asked you to complete the microbusiness, this will be due to the size of your organisation and/or the scale or risks around data processing.

Definition of a microbusiness

A microbusiness is small company that usually employs between 2 and 10 staff and a turnover of less than €1m and would have limited funds to employ their own Data Protection or ICT staff.

What are we looking for?

- Be accurate and transparent in your response.
 - Ensure that you have up to date Anti-Virus/Anti-Malware End Point Protection.
 - Overall level of data protection awareness and compliance measures in place.
 - No excessive collection or retention of Arts Council data.
 - Sufficient measures in place to ensure the confidentiality and integrity of Arts Council data.
 - No Arts Council Data is to be exposed to AI Agents.
- All cloud hosted services are secure, with data stored within EEA and have MFA enabled.
 - Data transfers to non-EU countries have a mechanism for which to do so and appropriate assessments have been carried out.
 - Separated Work and personal spaces e.g. iCloud segregated.

Instructions for Micro Data Protection and Information Security Assessment

Please ensure to complete the table on page 2 with details of the engagement e.g., your name, contact details etc.

What applications or software platforms, including any AI tools, do you use?

This is a list of any other parties/software etc that you will be using for operations on Arts Council data. Please complete this box fully with all parties listed. This should mirror parties you list in the Data Processing Agreement on Page 11.

Does the service or product you provide engage or share data with any AI Engine, i.e.

Generative, Agentic or any other machine learning service? If so, please provide detail?

Please indicate whether your organisation is using any products or services that incorporate Artificial Intelligence (AI), or whether you engage with any AI platforms or engines (for example, Microsoft Copilot, ChatGPT, or similar tools).

If AI tools are used, please outline:

- The nature and purpose of their use;
- Whether Arts Council data is processed, accessed, or made available through these tools, and if so, what controls are in place to protect that data; and
- Whether AI is used to support or inform any decision-making processes involving staff, applicants, customers, or other stakeholders, and the extent to which human oversight is applied to such decisions.

Where is your/our data stored?

Please include all locations that data will be stored. This will include physical and digital storage as an example: physical files in office, cloud back-ups in Microsoft data centres in Frankfurt and Dublin, Adobe cloud in Ireland etc. Please provide as much information here as you can.

What data do you store that is pertinent to the Arts Council? Do you share data Arts Council data with anyone else or other third parties?

Please include here the data that you will be processing for the Arts Council, for example artist CVs and application forms, financial information etc.

Please include if in the course of your work for the Arts Council there will be data sharing with other parties. This would include contractors under your employ, fourth party sub-processors such as another company that you utilise to carry out the work etc. If you are sharing data with parties outside of your own organisation, please provide as much detail as possible here, and include what the arrangement is (e.g., are they under contract, what Arts Council data will be shared with them etc).

[The next section of questions are only to be completed where you are a microbusiness / individual or sole trader. If you are an advisor and/or assessor, you don't need to complete the next section as the Arts Council will generally be providing you with data and will have knowledge of the type of data we are providing you with.](#)

What is the nature of the data you will be processing? (Editable list including Personal data Special Category Data, Data relating to criminal offences and convictions, no personal data being processed)

Please select the relevant type of data you will be processing (e.g., using, storing etc) on behalf of the Arts Council. You do not need to provide details of what the data is here, only select the relevant choice from the list (e.g., personal data).

- Personal Data: This includes any data that can be used to identify an individual e.g., names, email addresses etc).
- Special Category Data: This is more sensitive personal data and includes data listed in the box below such as health data).
- Data relating to criminal offences and convictions: This is where you would be processing data about criminal convictions.
- No personal data: This is where there is no data being processed that can identify an individual. For example, if you are working with survey results that are anonymous.

What categories of personal data are being processed? (Editable list).

Please select the relevant type of data you will be processing (e.g., using, storing etc) on behalf of the Arts Council. You do not need to provide details of what the data is here, only select the relevant choice/s from the list.

- Identification Data (e.g., names, ID cards, passports).
- Contact Data (e.g., email address, phone numbers).
- Communications Data (e.g., email communications, text messages).
- Web Data (e.g., website views, web forms).
- Log Data (e.g., back up logs).
- Physical characteristics Data (e.g., data relating to health and other physical characteristics).
- Finance and Tax Data (e.g., bank and financial statements, PPSN, funding histories).
- HR Data (e.g., CVs, contracts, other records of employment).
- Performance Data (e.g., records of employee performance).
- Location Data (e.g., IP addresses, Eircode).
- Social and Marketing Data (e.g., social media handles, records relating to marketing campaigns).
- Photography and Video Content (e.g., recordings of events, images of individuals).
- CCTV Data (e.g., CCTV footage).
- Voice Recording Data (e.g., an application being utilised where an individual's voice is recorded, video recordings where individuals' voices are being recorded).
- Other [Please list] (e.g., any other type of data not listed above).

What Special Categories of Personal Data are processed? (Editable list).

Please select the relevant type of special category data you will be processing (e.g., using, storing etc) on behalf of the Arts Council. This is personal data that is considered more sensitive in nature. You do not need to provide details of what the data is here, only select the relevant choice/s from the list.

- Health information (e.g., medical certificates and health records).
- Political opinions (e.g., information that provides for an individual's political opinions).
- Race, Ethnic Origin (e.g., nationality listed on documentation).

- Biometric Data (e.g., fingerprints, retinal scans)
- Membership or activity in a trade union (e.g., union registration number).
- Sexual Orientation, Sexual Preferences (e.g., records that identify an individual's sexual orientation or sex life).
- Religious or philosophical beliefs (e.g., dietary requirements can infer religion).
- No Special Category Data (e.g., where there is none of the above).

Who can I/we contact if we have questions about this assessment?

You can contact the Arts Council's Data Protection team by emailing dataprotection@artscouncil.ie.