**DBT MUSIC EXPORT GROWTH SCHEME: PRIVACY NOTICE**

The British Phonographic Industry (BPI) is responsible for managing and delivering the Music Export Growth Scheme (MEGS) and will run an application process to support grant awards. The Department for Business and Trade (DBT) has overall financial accountability for the scheme.

BPI will collect personal information from businesses applying to MEGS which will be shared with DBT.

DBT is committed to protecting the privacy and security of your personal information. This Privacy Notice describes how we collect and use personal information about you in accordance with data protection law, including the General UK Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018.

This notice is provided to meet the requirements of the UK General Protection Regulation (GDPR) and Data Protection Act 2018 (DPA) to provide transparency in how we process and use personal data collected from BPI, and your rights. It is made under Articles 13 and 14 of the GDPR.

This notice is supplemented by our [main privacy notice](https://www.great.gov.uk/privacy-and-cookies/)  which provides further information on how DBT processes personal data, and sets out your rights in respect of that personal data.

Data protection principles

DBT will comply with data protection law. This means that the personal information we hold about you must be:

* used lawfully, fairly and in a transparent way.
* collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
* adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
* accurate and kept up to date.
* kept in a form that identifies you for only as long as necessary for the purposes we have told you about; and
* kept securely.

The kind of information we hold about you

Personal data is information that relates to an identified or identifiable individual and only includes information relating to natural persons who:

* can be identified or who are identifiable, directly from the information in question.
* who can be indirectly identified from that information in combination with other information.

DBT will receive data from the BPI regarding MEGS applications and payments, including:

* identity of grant recipient.
* business name and contact details.
* unique identifier, for example national insurance number, unique taxpayer number, self-assessment number, VAT registration number; and
* details of grant provided and payment details.

Some businesses, sole traders and partnerships trade under an individual’s name. In some cases, the trading name and business address and postcode may be considered personal data.

Due to our role as a government department with responsibility for funding the grant scheme, we may also hold data including:

* high level aggregate data about the take-up of the grant scheme
* the performance of BPI in processing payments to businesses

Sources

We are collecting relevant personal data from the BPI.

Purpose

DBT will handle personal data collected across the MEGS scheme for the purposes of:

* monitoring the performance of the scheme.
* ensuring that grants have been paid out in line with the eligibility and subsidy allowance conditions for the scheme.
* evaluating and reviewing the impact, performance and costs of the scheme.
* researching the effectiveness of the scheme and supporting future policy development; and
* preventing and detecting payments in error and fraud, and taking action to mitigate the risk of loss in relation to fraud.

How we use your information

We will only use your personal information in accordance with data protection law. Most commonly, we will use your personal information where:

* we need to comply with a legal obligation
* it is necessary for the performance of a task carried out in the public interest or in the exercise of our official authority as a government department, including the recovery of any grant funds incorrectly awarded or paid
* it is necessary for the purposes of the prevention, investigation, detection or prosecution of criminal offences including fraud

In limited circumstances we will ask you for your consent to use your personal information, but your consent is not required if any of the above apply.

Situations in which we will use your personal information

We will also process your personal data (as the grant recipient) in the following circumstances:

* when carrying out any of our lawful functions
* to check the data we hold about you is accurate and up to date
* to compare it against other information to help combat fraud and crime
* when investigating an offence, engaging with parties to the investigation, including evidence gathering, fulfilling disclosure obligations and discussions to agree appropriate outcomes
* for case management, including evidence analysis and storage in line with statutory obligations
* to prevent, detect or prosecute a crime
* to bring civil proceedings and/or debt recovery as the organisation providing the grant funding
* to undertake statistical and analytical analysis
* to respond to questions sent to the department (such as from Parliament and Select Committees)

In addition we will process the data received from BPI to:

* analyse and review the take up, impact, performance and costs of the grant scheme.
* research the effectiveness of the grant scheme and support future policy development.
* prevent and detect crime; including the use of fraud analytics to look for unknown or undetected criminal patterns and behaviour.
* to take action to mitigate the risk of loss in relation to fraud against a public authority including:
	+ preventing, detecting, investigating and prosecuting fraud
	+ bringing civil proceedings as a result of fraud
	+ taking administrative action in connection with fraud

Legal basis of processing

Where DBT processes personal data for non-law enforcement purposes, the processing will fall under the UK GDPR and the Data Protection Act 2018 (DPA 2018). There are a number of requirements listed in the DPA 2018 to ensure this is lawful.

To carry out this function, the lawful basis by which DBT will process personal data is that the 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 data controller (public task, see Article 6(1)(e)).

This could include the exercise of a function of the Crown, a minister of the crown or a government department; the exercise of a function conferred on a person by an enactment; the exercise of a function of either House of Parliament; or the administration of justice.

DBT is also considered a competent authority and may process personal data for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Data sharing

We will not share your information with any third parties for the purposes of direct marketing.

DBT may share your data with third parties acting as data processors for DBT. These include:

* data analytic companies to support the Department in completing appropriate checks to ensure an applicant business is eligible to receive grant support under MEGS
* debt collection agencies and credit reference agencies to enable them to pursue debts on our behalf, and
* external research organisations that will be independently assessing the impact of the grant scheme.

We will have contracts in place with all third parties and they cannot do anything with your personal information unless we have instructed them to do it.

In some circumstances we are legally obliged to share information. For example, we might also share information with other regulatory bodies in order to further their, or our, objectives. In any scenario, we will satisfy ourselves that we have a lawful basis on which to share the information and document our decision making.

Where required by law, information relating to individual MEGS payments (which may include amongst other details the identity of the grant recipients and size of grant) will be shared by a granting authority on the UK’s public transparency database to enable compliance with the UK’s international subsidy reporting requirements with regards to the UK-EU Trade and Co-operation Agreement, World Trade Organisation Agreement on Subsidies and Countervailing Measures and other Free Trade Agreements.

In addition to sharing data with debt collection agencies, credit reference agencies and commissioned research organisations, DBT may also share your data with:

* law enforcement agencies both in the UK and overseas
* regulatory bodies
* anti-fraud organisations
* other government departments

We will only share your personal data with a third party where there is a lawful basis permitting the disclosure.

Data sharing for fraud prevention purposes

**Disclosure to a specific anti-fraud organisation – Serious Crime Act 2007**

DBT may disclose information to a specified anti-fraud organisation (SAFO) for the purposes of preventing fraud.

Section 68 of the Serious Crime Act 2007 was introduced as part of the government’s commitment to preventing fraud. It enables public authorities to disclose information for the purposes of preventing fraud, as a member of a SAFO or otherwise in accordance with any arrangements made with such an organisation. A SAFO enables or facilitates the sharing of information for the prevention of fraud and is specified by an order made by the Secretary of State. Disclosures of information from a public authority to a SAFO are subject to a code of practice and this, along with a full list of SAFOs we may share information with, is available on GOV.UK: Data sharing for the prevention of fraud: code of practice. In addition, all disclosures must be made in accordance with data protection legislation.

**Disclosure of information to combat fraud against the public sector**

Section 56 of the Digital Economy Act 2017 enables public authorities to share information in order to take action in connection with fraud against a public authority. This type of information sharing helps us to improve our ability to identify and reduce the risk of fraud against the public sector and recover public sector funds.

Fraud in this context means a fraud offence which involves loss to a public authority, or the exposure of a public authority to a risk of loss.

Taking action includes preventing, detecting, investigating and prosecuting fraud, bringing civil proceedings, and taking administrative action as a result of fraud.

Where DBT has entered into information sharing under this power, it has taken steps to ensure that information sharing proposals are balanced and proportionate and come under an appropriate level of scrutiny. This includes ensuring that such arrangements are set out in appropriate information sharing agreements.

We only use personal information shared under this power for the purpose for which it was disclosed, unless certain exceptions apply including:

* if the information has already lawfully been made available to the public
* the prevention or detection of crime
* for the purposes of a criminal investigation
* for the purposes of legal proceedings (whether civil or criminal)

DBT undertakes fraud analytics in respect of data from all grant’s applications (company name and registration number, trading name, post code and lender demand date) for the purpose of quantifying and/or identifying fraud and to look for potential fraudulent behaviour, patterns and trends. This activity is not limited to those applications where potentially fraudulent or suspicious activity has been identified.

As part of the fraud data analytics programme, we share grants data with the Cabinet Office to match it with other government data sets. The results of this will be shared with DBT, other government bodies and law enforcement agencies as appropriate.

Data security

We have put in place measures to protect the security of your information.

If required, our third-party service providers will only process your personal information on our instructions or with our agreement, and where they have agreed to treat the information confidentially and to keep it secure.

We treat the security of your data very seriously. We have strict security standards, and all our staff and other people who process personal data on our behalf get regular training about how to keep information safe.

Where possible the personal data is minimised, aggregated, or anonymised, for example in reporting performance, estimated losses and so on.

We have put in place appropriate technical, physical and managerial procedures to safeguard and secure the information we collect about you.

In addition, we limit access to your personal information to those persons, or agents who have a business or legal need.

We have put in place procedures to deal with any suspected data security breach and will notify you and the regulator of a suspected breach where we are legally required to do so.

All organisations we work with are required to agree to move, process and destroy data securely, in line with the principles set out in HM Government Security policy framework, issued by the Cabinet Office, when handling, transferring, storing, accessing or destroying information.

Retention of your personal data

Personal data is retained in accordance with the DBT retention and disposal policy. We, and third parties we share it with, aim to retain your personal information for only as long as it is necessary for us to do so for the purposes for which we are using it and in line with our retention and disposal policy.

In some circumstances DBT will anonymise your personal information so that it can no longer be associated with you, in which case we will use such information without further notice to you.

Your data protection rights

Under data protection law, you have rights we need to make you aware of. The rights available to you depend on our reason for processing your information.

Your right of access: you have the right to ask us for copies of your personal information. This right always applies. There are some exemptions, which means you may not always receive all the information we process.

Your right to rectification: you have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete. This right always applies.

Your right to erasure: you have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing: you have the right to ask us to restrict the processing of your information in certain circumstances.

Your right to object to processing: you have the right to object to processing if we are able to process your information because the process forms part of our public tasks, or is in our legitimate interests.

Your right to data portability: this only applies to information you have given us. You have the right to ask that we transfer the information you gave us from one organisation to another, or give it to you. The right only applies if we are processing information based on your consent or under, or in talks about entering into a contract and the processing is automated.

Automated decision making

Personal data collected by DBT will not be subject to automated decision making.

International transfers

Personal data will be processed in the UK. Your personal data will not be transferred outside the UK and European Economic Area (EEA), or by an international organisation.

DPO:

You can contact DBT’s Data Protection Officer (DPO) by contacting data.protection@businessandtrade.gov.uk

Complaints

If you think that your personal data has been misused or mishandled, you may make a complaint to the Information Commissioner, who is an independent regulator. The Information Commissioner can be contacted at:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Email casework@ico.org.uk

Telephone 0303 123 1113

Any complaint to the Information Commissioner is without prejudice to your right to seek redress through the courts.

Changes to this privacy notice

We keep our privacy notices under regular review. If there are any changes, we will update this page to tell you, for example, about any new uses of personal data.

Check this page to make sure you are aware of what information we collect, how we use it and the circumstances in which we may share it with other organisations.

From time to time, we may also tell you in other ways about the processing of your personal data.