

Data protection for artists

May 2020

This resource has been adapted from blog post 'The importance of data protection to artists' by Naomi Korn Associates, December 2019.

When processing data we are processing the details of a person's life and so care should be given as if the details are our own.

If you are an artist working in the UK, it's vital that for any personal data you collect, be it from buyers/customers, other artists, galleries, commissioners, employers etc. you must store their personal information securely to ensure you are safeguarding their information in line with the Data Protection Act 2018, the UK's implementation of the GDPR.

What is the GDPR?

The GDPR is the 'General Data Protection Regulation' and it came into force in the UK on 25 May 2018 as the Data Protection Act 2018. The GDPR harmonised data protection rules across EU member states. It applies to processing carried out by individuals and organisations operating within the EU, but also applies to organisations outside the EU that offer goods and services to EU citizens. The GDPR significantly enhances the rights of data subjects in the processing of their personal data. Data Protection laws are nothing new. In the UK, we have had data protection laws since 1998 (Data Protection Act 1998). GDPR is an uplift on existing data protection laws therefore.

Complying with Data Protection

Individual artists working as sole traders or small businesses who handle personal data must comply with the law.

Top tips:

1. Understand what personally identifiable data is - this includes the collection of names and addresses, contact details including business emails etc.
2. A privacy statement should be published on your website to communicate how the personal data is processed.



3. It is vital to keep a record of how information is handled. This is a basic part of day to day business. It does not have to be onerous or a chore but a key element in managing other's information with respect and showing that it matters to you. Reputations for good service are built on this. See ICO's website for guidelinesⁱ.
4. Data protection issues will affect all types of carriers of personal data – not just digital. This will include paper records, photographs, sound recordings, films etc.
5. Rights and privacy know-how nearly always mean contract know-how too. Putting in place robust contracts with third parties and/or making sure you understand what you are signing is crucial for ensuring compliance.
6. Not all data breaches need to be declared to the ICO, but it is vital that no matter what, you have sensible data breach policies in place to record any that happen. Breaches to be declared to the ICO include any loss or theft of personal data that could potentially cause harm or distress to the individual concerned.

Key Data Protection facts

- There is lots of over reaction to the new laws. Ignore instructions such as “all personal data must be deleted from emails”, “you must delete someone's records if they have not responded to your requests to confirm twice”, “you must delete all records of people who have resigned”, “delete all electronic records, but manual records are OK”, “you must always ask for permission before you can hold someone's personal data”. These and many more are nonsense.
- Data Protection laws apply to print and digital forms of personal data. Know what you have, why and where it is stored. Decide if you should keep it or not, and if so, make sure you plan how you keep it safe.
- Get the facts about when you may process, i.e., obtain, record, manage, structure, store, amend or delete, or disseminate personal data. The reasons can be found here on the ICO's website.ⁱⁱ

What is defined as 'Personal data'?

By UK law the definition is:

“Any information relating to an identified or identifiable natural person in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.ⁱⁱⁱ

What is a data breach?

‘A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.’^{iv}

As part of GDPR you have a responsibility to report certain types of personal data breaches to the relevant authorities and you must do this within 72 hours of becoming aware of the breach where feasible. More information about breaches you need to report and breaches you don't, see the ICO's website.^v

ⁱ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/>

ⁱⁱ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/>

ⁱⁱⁱ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/>

^{iv} <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>

^v <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>



© Naomi Korn Associates, 2021. Some Rights Reserved. This resource is licensed for use under a Creative Commons Attribution Share Alike Licence (CC BY SA)

Disclaimer: The contents of this resource are based on the assessment of Naomi Korn Associates Ltd at the time in which the resource was created (May 2020). The contents should not be considered legal advice. If such legal advice is required, the opinion of a suitably qualified legal professional should be sought.