ARTLOGIC

GDPR compliance roadmap for art businesses

Introduction

The General Data Protection Regulation passes into law in every EU country on 25 May 2018. It clarifies and strengthens existing legislation. It enhances the rights of data subjects and extends the definition of personal data. It obliges organisations who keep and use personal data to be more accountable as well as the companies that provide services to help manage personal data.

Not only do all businesses of every size have to be compliant, they have to be able to demonstrate compliance, in terms of evidence, audit logs, written policy, records of training and supplier contracts. Some firms in the EU (though not most art galleries) will need to register with the regulatory authority in their respective country (the ICO in the UK).

This document contains no information about the law itself. We assume for the purpose of this document that the reader already has a working knowledge of the law. Many resources exist to help you become familiar with the law and its implications. Your lawyers, and any trade bodies to which you belong may be able to offer guidance. Knowing the law does not make it easy to figure out how to get started.

This document is intended to suggest some steps you might need to take on your journey to compliance and offer an overview of tasks you will need to accomplish across your business.

Phase One: Policy and planning

Appoint leadership

Someone at the most senior level of every business should assume leadership in the area of data protection. This person will need to command resources, map out policy, delegate responsibility. They will not only help avoid the risk of fines and reputational damage that could destroy the business, they will help it to derive operational benefits. The business response to the challenge needs to be proportional to its size and resources and the type of data being processed, so it will be up to the leadership to consider the risks and your attitudes to them.

Work out what Personal data you have

Identify what types of personal data you process, where that data is held including all the systems you use (paper and electronic, backups, archives), who has access to which parts of it or all of it (identify the teams and access levels not individuals), for what purposes it is used, check whether only the minimum data is being kept and if it is retained longer than necessary. As a minimum, this will include your payroll, staff records, marketing database and invoices. Start with the most widely used and most confidential. Consider how old the data is. Identify where it is physically, including cloud based services, cloud based backups, employees' personal machines, backups, etc. A template from the ICO website for starting your Information Asset Register is available here: http://www.nationalarchives.gov.uk/documents/information-management/iar_template.xls

Create policy

Identify the lawful basis or bases for the different types of data you are processing and how they fit with the purpose/s for which data is collected and processed. Your whole approach depends on this. Think about your future needs. If you decide to use the data for a different purpose and consent was your legal basis for holding the information, you may need to seek fresh permission.

Establish a clear Privacy Notice, explaining the purposes, retention periods and lawful bases for processing data and make sure that this is available. Be clear in this policy where consent is not needed and what use is made of a subject's data. The policy should be clearly communicated to its respective audiences and available on your website. You may need a lawyer to help you make this.

Appoint a Data Protection Officer

In public organisations, and for some private companies it is a legal requirement to appoint someone to this role. Even without someone bearing this job title, someone needs to be in charge of updating information, revising service provider contracts, training staff, implementing policy on retention and access and responding to public requests for data.

Raise awareness

Start to raise awareness in the organisation about any gaps which need filling, the areas that are being worked on and the procedures and policies that might need most urgent change.

Phase two: Getting to grips with the data

It makes sense from a customer relationship and reputation point of view that, if anyone requests to see the information you keep on them, or lodges a complaint, that you are only storing the data that they would expect and that you are processing it for a legitimate reason.

Artlogic Contacts Database

There is no need to look at every field and every contact record to get to grips with your data but you may need to give some records consideration to identify how long someone has been in your system, how much you know about them, the purpose for your keeping their details. In order to help you focus your attention on the records which matter most, you can use our data protection tools. For each record, you can see the special classification options in the data protection part of the contact record when you are editing - just scroll down below the contact details. Naturally you can set these values using the Update Multiple records function.

- The selector will automatically be set to indicate that a contact is a client if they have been invoiced via Artlogic but for historic records we have imported this will not happen and there may be other reasons why you need to set this manually, for instance if there are multiple contact records for the same person.
- Set the value to be 'supplier' for your supplier records and flag your 'professional contacts' for journalists, curators, advisors, etc. These groups should still be able to opt out of your marketing lists but there should not ever be an issue with you storing / processing their details.
- Having identified your existing customers, your suppliers and your professional contacts, nearly everyone else on your database is going to be a marketing lead and, providing they supplied their personal details (business card, visitors' book, website sign up, enquiry form) they are regarded as a soft opt-in to your marketing list. As private individuals rather than representatives of a company, GDPR gives individual consumers enhanced rights but you do have a right to market to people who have provided their details, who know why you are processing them and have the means to opt out. Focus on this group to look for duplicated, outdated, inaccurate or unnecessarily sensitive information and remove data or delete old records. If you have been mailing someone for ten years and they have never been in touch or bought anything, you may not want to keep their data. You can distinguish between those who supplied their details anonymously (web forms, visitor's book, etc.) or those who gave you their details more personally via email / phone / art fair enquiry, exchange of business cards, etc. New website sign-ups will automatically show the flag that they gave you their data anonymously.

Statistics about the numbers of these groups and a link to find each group will show on the GDPR dashboard which you can find in the Data Protection menu item under Contacts.

If your business is based outside the EEA, you might want to focus more closely on your contacts inside the EEA as far as GDPR is concerned. Artlogic has a view of the contacts database showing you only records inside the EEA. To make sure that this is effective, ensure that every contact has a country value and that the country names are consistent.

Marketing list

Having identified who you are mailing and maybe before you have finished removing some old contacts, most firms will probably need to get in touch with everyone before 25 May 2018.

There has been a lot of panic and misinformation about what people should do with their marketing database. The advice we have received about marketing lists runs as follows:

Do not seek to obtain or renew consent to be on the mailing list for your existing contacts. If your valuable contacts did not provide consent, you would definitely break the law if you continue to market to them and you may lose a high proportion of contacts from your list. Furthermore, if it appears that you are attempting to secure consent which is not fully compliant, you will be breaking the law to seek consent by email. So what should you do instead?

Make sure that you have a well written Privacy policy on your website as soon as possible that fully and clearly explains the purpose/s for which you keep data, what data you keep and how it is collected and the retention period (until they opt out). You should warn people that you may process their details outside the EU but will ensure that you have made adequate operational and technological provision to ensure that their data is held securely. You need to do this because of the way Artlogic processes your data with multinational service providers and so you can access Artlogic data from offices outside the EU or when you are travelling.

Your system administrator needs to add the address of your privacy notice web page to the preferences using the field for this in Admin > Preferences to make it appear in your mailings.

Send a mailing to your marketing list to inform them of the new privacy policy with a link to read it. For clients, suppliers and professional contacts, you should ensure that they have the option to stop receiving marketing communications. Luckily the Artlogic mailing system adds links in the footer of every message and these enable recipients to read the privacy policy and change their communication preferences. Our 'unsubscribe' link is now 'update my preferences' and this will enable recipients to choose between different types of communications. They can choose to receive sales emails (offers), more personal invitation messages and the less personal blasts about exhibitions, art fairs, newsletters, etc.

Cleaning up

Across all your data systems, you should identify and consider deleting all the personal data you don't need or cannot justify. For systems other than your Artlogic contacts database, this includes all storage of obsolete information, backups, downloads, 'just-in-case' copies on all the file systems of company computers, personal computers, hard disks, cloud providers, cloud storage, pen drives and mobile devices. You may want to delete data where its origin or purpose, is unknown.

Across all your online systems and the file systems of all your computers, try and locate the bad data records (kept beyond its necessary retention period) mixed in with current data (such as former clients, former employees, etc.). Within records, is there any data that is not aligned with a stated purpose understood by the data subjects?

Is there any special category data for which you have no consent, for example on religious beliefs, sex life, sexual orientation, biometric data, criminal convictions or political affiliations? You should consider deleting all special category data. You should definitely consider either deleting all data about children or seek special advice about how to store this legally.

It may seem obvious but do not store bank or credit card information anywhere except in a financial system.

Don't forget that any searchable system like email or a paper file system needs consideration including old documents, contracts, invoices and employee records that are no longer needed for practical purposes.

But be careful not to go overboard as there are some details you are required to keep for years after they are relevant, either for legal reasons, for instance sales, employee records, anti-money laundering checks or for resolving disputes, for instance, customs paperwork, shipping manifests.

If you use consent

Where consent is being sought, ensure that the mechanism for gathering consent is specific, informed and unambiguous, created by an affirmative action (ticking a box and then pressing submit) and freely given (not part of an offer or conditional in any way). You will need consent for each purpose and to record all responses so that mistakes are not made and you must keep an audit trail. You will also need consent for each method of communication (email, SMS, phone).

Phase three: Process and paperwork

Follow up all third party vendors

From the Information Asset Register created in the previous step (see page two), work out who all your third party vendors who act as processors. Check that the data is being processed lawfully and obtain and record copies of all the contracts for these suppliers.

Create a data breach response process and then test it.

Establish clear policy and rules regarding who would responsible for data breach management, how the relevant people contact each other in a hurry, how you report a breach to the ICO, how you investigate a breach, how you communicate with your clients and your data processors. Does your data processor have updated contact details for designated data protection officer and their deputy, should they be out of contact?

Put policies, procedures and personnel in place

- Make sure that retention periods are established, communicated and enforced by humans or systems.

- Where multiple systems record data exist for the same individual, try and create processes to update one from the other or reduce the number of systems so that requests for deletion or updates are more efficient and failsafe.
- Consider if you need to verify individuals' ages in sign up forms to avoid storing details about children.
- Implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities and reviews of internal HR policies. Conduct data protection impact assessments for major systems and any new ones you are considering. See below for a useful link about contracts and more about audit paperwork advice from the ICO.
- See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

Work out how to process Data Subject requests

You must develop mechanisms or people-based systems to enable data subjects to:

- be able to obtain copies of the data you hold about them. In Artlogic, you will be able to report on any individual from the data inside Artlogic but that will not supply data from other systems, like your email or any external CRM, mailing system.
- be able to correct inaccurate data across multiple systems
- erase data upon request and decide if this should apply to any backups, duplicates, records in other systems. Be aware that you may need to keep for statutory purposes (or want and be entitled to keep) information about former clients, people who have asked not to be contacted (suppression lists), so you should consider what information is removed or reduced if someone requests to be 'forgotten'. Artlogic is adapting our process for revert deletions which will reapply any request to be deleted or not to be contacted.
- make data portable typically in an electronic data format. This right is a less important consideration as, unlike a customer moving from Tesco to Sainsbury and wanting to take their grocery list with them, clients do not move from one art gallery to another so there is no standard electronic formats for transferring data. You can export key contact data into a spreadsheet and send it as CSV, which is a common data interchange format.
- record and execute people's preferences to change contact preferences and methods or have data reduced or rendered inactive or deleted – however data may not just exist on a database, it may be social media interactions, email, documents, etc.

Security

Security is one of the core principles and being lax in this area could expose companies to large penalties found to be negligent. You should review **and document** your security procedures, including physical security, access levels, access to all your online systems, bulk data handling.

Security features of Artlogic

Artlogic uses the latest cloud infrastructure to protect your data. It is atomised and encrypted across a sophisticated cloud system that is fully resilient. This is more secure, scalable and resilient way of doing things than we could operate using our own equipment. The data is encrypted in transit using 256 bit TLS v1.1 or v1.2.

Features you should use

- We suggest that you only give your database users access to edit and download only the data they need. You decide on privileges per user, including preventing downloading ANY lists of contacts, restricting the number they can export.
- You can restrict off-premise use by restricting access to the system for some users to one or more networks using IP restriction.
- We strongly recommend use of Two Factor Authentication, requiring users to using a code on their phone to unlock Artlogic as well as their password.
- Passwords should be really strong and rotated every few months. Never share your passwords with colleagues or with other systems.

General IT security

- Make sure that you keep your operating system up to date on your servers, desktops, laptops and mobile devices.
- Make sure that your computers have login passwords, timeout screensavers, secure backups (encrypted if possible).
- Make sure you never send passwords, personal details, banking details via email.
- Make sure that you have secure email provider.
- Make sure that you have anti-virus, anti-malware software installed and kept updated and that everyone is cautious about clicking on links in emails or on dubious websites.

Training

Provide initial and then regular training to everyone about the law, how you use data (purposes, policy), about your company's policies, breach prevention and reporting process, who has access to what data and the use of security measures that should be taken with bulk raw data. You should also provide regular training about IT security and the security features in Artlogic.

Next steps and further reading

Resources

View https://artlogic.net/gdpr for details about what Artlogic has been doing and to read any other resources.

Legal advice

You may want to take some legal advice.