How will the General Data Protection Regulation Impact the Art Sector?

Ian De Freitas | 20 October 2017

The EU General Data Protection Regulation represents the biggest change in European data privacy laws in twenty years. The purpose of this article is to explain in very straightforward terms what GDPR means for galleries and auction houses and the steps that the sector needs to take to be ready by May 2018 when GDPR takes effect.

> "The new regime seeks to empower individuals, putting them in control of their personal data."

What is GDPR?

GDPR is a new regulatory regime affecting how organisations manage personal data relating to living individuals. So that would cover data you hold about your clients and customers, staff, volunteers and supporters and suppliers, amongst others.

GDPR very much strengthens EU data protection laws and adopts a pro-privacy stance. As the present regime is based on legislation dating back to 1995, GDPR also focusses on modernising the law to make it fit for the 21st Century.

The new regime seeks to empower individuals, putting them in control of their personal data. Organisations will need to embrace the concept that they effectively hold personal data "on-loan" from individuals.

GDPR also seeks to export the EU concept of data privacy globally, directly regulating many more organisations based inside and outside the EU. For example, it catches for the first time businesses based in America which are processing personal data of clients and customers located in the EU in the context of supplying services to them.

To convey the message that data protection must now be taken seriously, GDPR introduces fines and other sanctions that have the potential to hit non-compliant organisations very hard and disrupt their core operations.

In summary, GDPR requires a culture change in most organisations. In the past, the collection and use of personal data has been seen as relatively low risk. Having a lot of personal data was seen as potentially useful, for example in understanding what clients and customers might want. However, because of the strengthened rules and higher sanctions if you get things wrong, you cannot adopt these attitudes anymore. The problem is that this approach has been deeply ingrained in organisations for years and the clean-up of old and risky data is likely to take considerable time and effort.

When does GDPR take effect?

GDPR will apply from 25 May 2018. It is a Regulation, meaning it takes effect

automatically without enabling legislation at a national level. However, some aspects of GDPR are being left to EU Member States to decide. The UK Parliament has just started considering a new Data Protection Bill designed to do this. Care should therefore be taken to check provisions at a national level.

GDPR adopts a "Zero Day" approach. This means that everything has to be compliant by 25 May 2018. Compliance with existing data protection laws may not be good enough to allow the processing of personal data after this date.

What are the Key Themes of GDPR?

GDPR is a complex piece of legislation. However, to understand it better, it can be stripped down to the following Key Themes:

1. Extending Individual's Rights

Individuals are given more rights, such as the right to require their data to be wholly or partly deleted. They also retain existing rights, such as Data Subject Access Requests where they can request an organisation to tell them what personal data is held about them. However, the requirement for the individual to pay £10 to exercise this right is being abolished.

Impact – organisations will need to have processes and systems that can effectively respond when these rights are exercised. This can involve a wholesale change to IT systems and database management.

2. Consent and Transparency

Rules on consent are tightened, meaning that opt-out consent (pre-ticked consent boxes) will no longer be good enough and opt-in consent will be the norm. Consent in the context of processing employees' data is unlikely to be valid at all. Organisations will also have to provide clearer and more concise explanations about what they are doing with individuals' data, and whether they are seeking consent or relying on another basis to use the data.

Impact – if organisations want to continue processing data after "Zero Day" they will have to re-permission data, or re-evaluate why they are processing the data and inform the affected individuals by amending and re-issuing privacy policies to clients and customers. With employees this is likely to involve a wholesale change to the privacy terms issued to them where consent has often been relied on in the past.

3. Accountability

Organisations will not only need to be compliant, but also able to demonstrate that they have taken all necessary steps in that respect. Some organisations will also need to appoint Data Protection Officers to help them with this, whose roles and responsibilities are prescribed in the new regulations. This seems unlikely in the galleries and auction houses sector however, as a DPO is only required where an organisation is processing large amounts of sensitive data or monitoring individuals as part of its core activities.

Impact – this greatly increases organisations responsibilities to maintain records of

data compliance and provide effective training to staff. If you do need a DPO, this new compliance role requires a range of skills that relatively few individuals are likely to possess. So find a DPO sooner rather than later.

4. Privacy by Design

Privacy must be built into products and services from the outset and not treated as an afterthought. This can extend to carrying out formal Privacy Impact Assessments on higher risk data processing activities.

Impact – organisations have to change the way they think about personal data and consider privacy as a key area of risk in everything they do. They may have to revise processes to make them less privacy intrusive.

5. Direct Regulation of Data Processors

Current EU data protection laws apply to data controllers, i.e. the organisations who decide how the personal data is to be processed. Now, the regulations are being extended to data processors, i.e. those who act under the instructions of data controllers when processing data on their behalf, such as Cloud data storage providers. Contracts between data controllers and data processors will also have to include very specific terms prescribed by GDPR.

Impact – controller/processor contracts will have to reflect this more direct and prescriptive level of regulation. Existing contracts extending beyond "Zero Day" will have to be re-negotiated. Risk allocation between controllers and processors will also need careful consideration, particularly in light of the sanctioning powers available to regulators.

6. Global Reach

Organisations outside the EU will now be directly regulated as GDPR adopts a "pay to play approach" – if you want to use the data of individuals based in the EU to offer goods or services to them or monitor their activities in the EU, you have to abide by the EU's data privacy rules.

Impact – organisations that have never been directly regulated in the past will now be so, and they will have to become familiar with EU data privacy concepts very quickly.

7. Mandatory Breach Reporting

For the first time all data breach incidents will have to be reported to regulators, and within seventy-two hours of the data controller becoming aware of them. More serious data breaches will also have to be reported by data controllers directly to the affected individuals.

Impact – Organisations must put in place data breach notification and reporting processes and be familiar with these to meet the time limits and the risks associated with reporting, not least the risk of subsequent investigations by regulators and compensation claims by affected individuals.

8. Sanctions and Powers

Regulators will have the power to levy fines of up to €20M or 4% of annual turnover (whichever is higher) for breaches of GDPR. They will also have the power to require data processing to stop until it is brought into compliance.

Impact – organisations have to treat personal data as a serious risk, both in terms of the effect on profitability and the ability of regulators to disrupt core businesses processes. This represents a big change in culture where previously the gathering and processing of large amounts of data has previously been seen as beneficial and low risk.

How will GDPR be enforced?

We predict that there will be three main ways that organisations will be targeted:

By national data protection regulators using pro-active auditing powers in data-rich sectors. We do not consider that the galleries and auction houses sector will be a pro-active target, at least not for the UK regulator, the ICO. More likely targets are IT platform providers (who might be suppliers to the sector), social media, financial services, insurance, hotels and retail;

National regulators may however use their powers in a re-active way as a result of mandatory breach reporting of major incidents or a series of less serious breaches indicating systemic risk in an organisation or sector;

By individuals investigating the use of their data by organisations and reporting non-compliance to Regulators. We think this is the most likely way that the galleries and auction houses sector will find itself under investigation. This is by its nature unpredictable.

Adverse findings by Regulators may also be followed by compensation claims by affected individuals. These follow-on damages claims are specifically encouraged in GDPR. Compensation claims can be brought merely for distress. Liability could be very significant where hundreds or even thousands of individuals are affected.

What steps should you take to progress towards compliance?

Each organisation needs to find its own way to compliance taking into account factors such as its current level of compliance, its attitude to risk and the level of compliance it wants to reach, and its culture.

However, a basic project plan to achieve a defensible level of compliance usually consists of the following steps:

Obtain senior management approval for the project and a sufficient budget;

- Appoint a team to lead the project, drawing in individuals from areas of the organisation such as HR, Marketing, Legal, IT and client facing functions. Consider and appoint a DPO if required;

- Investigate what personal data the organisation processes and how it comes in, moves across and leaves the organisation (often called Data Mapping);
- Review processes for compliance using the Data Map and carry out assessments on them to identify impacts on individuals' privacy, the impact on the business if processing is non-compliant and the steps needed to achieve GDPR compliance;
- Implement the steps needed to achieve GDPR compliance, such as updating policies and re-issuing them to affected individuals, refreshing consent, improving data security and IT systems, and re-negotiating controller/processor contracts;
- Train staff in the new policies, processes and procedures;
- Monitor compliance with the new policies, processes and procedures and enforce them where necessary or alter them where this is required.

And finally, does Brexit have any impact?

You may have noticed that this is EU legislation. Does Brexit therefore mean that you can ignore it? The answer is no. First, GDPR takes effect directly as an EU Regulation next May so it will apply in the UK before Brexit happens. Second, and more long-term, the UK Government actually likes GDPR and has decided that it will be retained post-Brexit. The Data Protection Bill introduced into the UK Parliament in September 2017 to supplement GDPR reflects this position.

So, we are afraid that GDPR is something that simply needs to be addressed, and soon if you have not already started.

If you require further information on anything covered in this briefing please contact Ian.defreitas@farrer.co.uk; +44(0)203 375 7471), or your usual contact at the firm on 020 3375 7000. Further information can also be found on the Disputes page on our website.