Guide to

GDPR 2018

GENERAL DATA PROTECTION REGULATION

A guide to the General Data Protection Regulation for art market businesses

- COMPLIANCE GUIDANCE
- CASE STUDIES
- JARGON BUSTER
- YOUR QUERIES ANSWERED
- RIGHT TO BE FORGOTTEN
- EMAIL MARKETING
- PRIVACY NOTICES

ANTIQUES TRADE gazette SUPPLEMENT

INTRODUCTION

Keep calm and prepare for GDPR

You may know about it already and are prepared, which is great. Or you have heard about it but aren't sure what it all means. We're talking about the much-hyped General Data Protection Regulation 2018, a new set of EU-wide rules that from May 25 will govern the way organisations gather and use people's details.

What does this scary-sounding regulation have to do with me, you may well ask. A lot, if your business captures information on buyers, clients, employees and companies you might work with.

Which is why you do need to get a handle on the GDPR and it is why *Antiques Trade Gazette* has produced this guide. We are not dispensing legal advice here, but rather have consulted expert sources to familiarise you with key aspects of the GDPR. The people quoted in this guide say that while concerns about the new rules are understandable, a common-sense approach to compliance is best.

If your business already complies with current data protection and digital marketing laws, chances are the GDPR will be a refinement rather than big bang, with better targeted marketing the real bonus.

However, should your firm be starting on the road to compliance, it is vital you gain awareness of the new rules and have a plan. Begin by asking yourself the questions posed in our 'Key steps' feature.

Whatever your firm's state of readiness, we hope this guide proves a useful and timely read.

Noelle McElhatton
Editor: Antiques Trade Gazette
editorial@antiquestradegazette.com

Publisher's note to readers

Please note this guide is provided as a background resource to help the art market understand the implications of the GDPR and the need to be compliant. It does not cover all the issues that may arise nor does it constitute any form of legal advice and should not be treated as a substitute for specific advice from a lawyer. Art market professionals are also referred to the ICO website (ico.org.uk) where more specific and detailed guidance is provided and a helpline offered.

CONTENTS

Editor: Noelle McElhatton
Publishing Director: Matt Ball
Designers: Gee Ibrahim, Justin Massie-Taylor

Editorial contact: +44 (0)20 3725 5520
editorial@antiquestradegazette.com

Advertising contact: +44 (0)20 3725 5500
advert@antiquestradegazette.com

Antiques Trade Gazette, Harlequin Building, 65 Southwark Street, London SE1 0HR. Tel: +44 (0)20 3725 5500
Printed by Buxton Press Ltd

Published and originated by Metropress Ltd trading as Auction Technology Group, publisher of ***Antiques Trade Gazette***

Visit the UK data regulator's website: ico.org.uk

GDPR at a glance

The rules around how firms handle customer data will change from May 25. Below includes key extracts from the guidance issued by the UK data regulator, the ICO.

Q What is GDPR?
A The General Data Protection Regulation is a new, EU-wide law that replaces the Data Protection Act 1998 in the UK. It places greater obligations on how organisations handle personal data. It comes into effect on May 25, 2018.

Q Why is it being introduced?
A The current legislation is 20 years old and pre-dates the huge increase in digital information about individuals. The GDPR aims to strengthen the rights of individuals regarding how personal data is gathered, stored and used by organisations and commercial businesses.

Q What's new in GDPR compared with current law?
A Essentially, consumers will have more control over how organisations use their data and there are greater responsibilities on firms to manage personal data. There are also bigger fines for misuse of data.

Q With Brexit, will GDPR apply to the UK?
A The UK's new Data Protection Bill integrates GDPR into UK law and is currently making its way through Parliament.

In addition, any organisation handling the personal data of EU citizens, and regardless of whether those organisations are based in the EU or not, is potentially liable to comply with GDPR.

Q How can I start preparing for GDPR?
A Read this *ATG* guide and also the latest guidance from UK data privacy authority the Information Commissioner's Office (ICO) on the GDPR at ico.org.uk. The information for small businesses on this website is very relevant to art market firms.

Q Will I always need a person's consent to process their data under GDPR?
A In short, the answer is no.

Consent of the individual whose data you hold is one lawful basis for processing, but there are others:

- **contractual**, where an individual has entered into a contract with a business, for example buying at auction or from a dealer;
- **legal obligation**, if you need to process data to comply with a law or statute;
- **legitimate interests**, which can include your firm's own commercial interests, balanced against the individual's interests and rights. GDPR states that using personal data for direct marketing purposes can be a legitimate interest;
- **vital interests**, where you need to process data to protect someone's life;
- **public tasks**, where processing is necessary for performing a task that is in the public interest.

Most lawful bases require that processing is 'necessary'. You must determine your lawful basis before you begin processing, and you should document it.

Jargon buster

GDPR defines **personal data** as any information relating to an identified or identifiable person (the 'data subject'). This is a much broader definition than that in the current law GDPR replaces in May, the Data Protection Act 1998. In the art market, any details you may hold of buyers, vendors, exhibitors and employees constitute personal data.

The **data subject** is the natural person (ie, a living individual) whose personal data you are processing.

Data processing means any operation or set of operations which is performed on personal data whether or not by automated means. This includes storing and extracting personal data from your customer database and using it for marketing purposes.

The **data controller** ('controller') is the person who decides the purposes and means of processing personal data. In the art market, this will typically be an auctioneer or a dealer, whether a sole trader or a limited company.

The **data processor** ('processor') is a person or company who processes personal data on behalf of the data controller. The GDPR primarily applies to controllers but also to processors. Many firms will use processors, for example, to store customer or HR data offsite or in the cloud, or to manage email marketing.

A **data protection officer** (DPO) is the person within a business mandated by the GDPR to deal with compliance and privacy issues. If you don't need to mandate one – and we expect many art market businesses won't need to – consider using another title such as data privacy manager if you wish to appoint someone to look after this area but don't want the DPO provisions of the GDPR to apply.

Consent in the GDPR means obtaining the agreement of the data subject to have their data processed. This consent must be freely given, specific, informed and unambiguous.

The **Information Commissioner's Office** is the UK's independent data privacy regulator, whose role is to uphold data privacy rights. As part of its remit, the ICO can fine organisations that breach data protection law. The new Data Protection Bill gives the ICO the power to issue higher fines than currently, of up to €20m or 4% of global turnover for the most serious data breaches.

Key steps to GDPR compliance

SIMON STOKES,
Partner, Blake Morgan

Simon Stokes is a partner with law firm Blake Morgan in London specialising in both technology law and art law.

He works with a number of art market clients including the Society of London Art Dealers (SLAD) and its members on ARR, copyright and data protection, as well as on consumer and commercial law.
blakemorgan.co.uk

The arrival of GDPR in May 2018 is fast approaching, so art market firms that haven't already done so should start preparing for the changes. **Simon Stokes**, partner at law firm Blake Morgan, charts the key measures that businesses need to take to be compliant

Though the first draft of the General Data Protection Regulation was published back in 2012, you would not be alone if your business is only now starting to prepare for the regulation that becomes law on May 25.

Those already in the midst of their compliance project should be checking to see how their action plans are progressing and whether all key issues are being addressed.

The best place to start your journey to achieve GDPR compliance is to ensure key stakeholders and decision-makers are aware of the issues and are committed to compliance, and that budget and resources are appropriately allocated. You should prepare to carry out an initial audit or information gathering exercise so you can document what personal data you hold, where it came from (and how it was obtained, for example whether privacy notices or similar were used), how you use this data and who you share it with.

Art dealers and auctioneers will certainly be processing personal data on customers and prospects (including unsuccessful bidders), for marketing as well as for transactional purposes, and on their staff and possibly business partners.

Having done this, you are then in the best possible place to take the actions you will need to take in order to achieve compliance.

Bear in mind too that GDPR compliance is an evolutionary process. No organisation ever stands still, as the Information Commissioner's Office in the UK (ICO) has recently stated: "You will be expected to continue to address emerging privacy and security risks in the weeks, months and years beyond May 2018."

Summarised in the following pages are some of the key changes under the GDPR, together with actions you can take now to help ensure that your business is ready. The tables use definitions taken from the GDPR which are summarised in the box on the previous page.

> Auctioneers and art dealers will certainly be processing personal data on customers and prospects

GDPR 2018
GUIDE TO NEW DATA PROTECTION RULES

ANTIQUES TRADE gazette

PRACTICAL STEPS

Key changes in the GDPR + Actions to take now

Being more transparent with individuals – customers, prospects and employees

The GDPR requires data controllers to give individuals more information at the time their data is collected – this includes explaining the legal basis of your processing (for example, their consent or your legitimate interests), your data retention periods (that is, how long you will hold the personal data) and that individuals have a right to complain to the Information Commissioner's Office (ICO).

There are additional obligations whenever you seek consent from an individual to the processing of their data. Bear in mind that your employees, other workers and consultants also benefit from the enhanced transparency required by the GDPR.

Review your customer-facing terms and your privacy policies – you already need to tell people why you collect their data and what you do with it. These are likely to need substantial revisions to meet the new requirements.

If you are relying on customer consent to legitimise your processing (for example, for email marketing), check that the method of obtaining consent will meet the new rules. Note that under the new GDPR rules, the data subject can withdraw their consent at any time and consent requires a positive opt-in. You cannot infer consent from silence, pre-ticked boxes or inactivity.

If you cannot rely on consent, ask yourself if you can rely on one of the five alternative conditions for processing (see 'GDPR at a glance', page 3).

If you employ people, don't forget your employees and other workers. You won't be able to rely on employee consent to process their data, so you will need to determine on what other legal basis you will process your employee data going forward.

Employees will require privacy notices and there are likely to be changes needed to your employment contracts and policies in order for you to comply with the GDPR. The processing of sensitive personal data (what the GDPR calls 'special categories of data') and criminal records are also subject to additional regulation and conditions under the Data Protection Bill 2017 (which will replace the Data Protection Act 1998) – for example, an employer may need to have an appropriate policy document in place if they process such personal data.

Demonstrating your compliance

An overarching theme of the GDPR is the principle of 'accountability'. There are new requirements on data controllers (and data processors) to demonstrate their compliance by fully documenting all their data-processing activities.

However, this obligation is more limited for smaller businesses (fewer than 250 employees).

The GDPR also makes 'Privacy by Design' a legal requirement. This means firms need to take data privacy into account when starting projects such as database builds.

Consider what records you keep of your decision making and your processing activities.

Can you demonstrate your compliance by pointing to staff training, internal audits of processing and reviews of internal policies, for example?

Review your contracts with processors to ensure that they meet the requirements of the GDPR.

If you don't already use them, think about introducing data protection impact assessments for new projects that involve the processing of personal data. These are a requirement of the GDPR where the proposed processing is high risk – for example, large-scale CCTV monitoring of public areas or collecting customer data for profiling purposes (for example, to predict bidder behaviour).

Note also that while GDPR does not require you to notify your processing to the ICO (as is currently the case), you will still need to pay the ICO an annual data protection fee. These fees are likely to range from £55-£1000 or so, depending on the size and nature of the processing of the organisations concerned.

Photo courtesy of W&H Peacock

PRACTICAL STEPS

Key changes in the GDPR	+ Actions to take now
Mandatory breach notification Controllers will have no more than 72 hours to report any data protection breach that isn't de minimis to the ICO. Where the breach is likely to result in a high risk to individuals, they must also notify individual data subjects without undue delay.	Review your internal systems to ensure that you can meet the new breach notification requirements. Review your processor contracts to ensure they contain obligations to report breaches to you. Bear in mind too the best place to be regarding security breaches is to avoid them. This means taking your IT security procedures very seriously, investing in and using secure systems including passwords and encryption, firewalls and current anti-virus software. It also means addressing the human element through training and procedures designed to minimise the risks of hacking, phishing and other cyber security breaches.
Appointing a Data Protection Officer Companies that process large volumes of data as part of their core activities (whether as a processor or controller) will in certain cases be required to appoint a 'Data Protection Officer', as will public bodies. This will be a statutory role (with appropriate employment protections), reporting directly into senior management, with specific functions set out in the GDPR.	Decide whether you need to appoint a statutory Data Protection Officer (DPO) – this is unlikely to be required for most auctioneers and dealers because of the relatively small size of their businesses and how they typically process personal data. It is good practice nevertheless to appoint a person responsible for data protection within your organisation. However, they should not be a called a 'Data Protection Officer' unless you wish to comply with the specific requirements for DPOs in the GDPR which may well be unduly onerous, especially for small businesses.
Much higher penalties when things go wrong Companies will face much stiffer penalties for non-compliance. Under the GDPR, the regulator will be able to issue administrative fines of up to the higher of €20m or 4% of worldwide turnover – a very significant increase on the current monetary penalties (which are limited to £500,000).	Ensure that the risk of penalties for non-compliance with the GDPR are fully understood at senior management and board level. Consider what measures you can take to reduce these risks. Review your processor contracts to ensure that liability is adequately flowed down.
Enhanced rights for individuals The GDPR includes a suite of rights for individuals or 'data subjects'. As well as subject access rights, which are retained from current law, individuals will have the right to receive their data in a commonly-used and machine-readable format. They will also have the right to have their data erased (called the 'right to be forgotten'), though the right to erasure is subject to certain exceptions. These include if an organisation has legal or regulatory requirements to retain data or if an employer needs to hold on to data and has lawful grounds for doing so.	Review your process for responding to subject access requests under GDPR where a person is entitled to request details of the personal information you hold about them and how it is being processed. You are obliged to supply this without delay, free of charge and in any event within one month. Make any changes necessary to comply with the new rights for individuals. Consider whether you need to change your communications with individuals to ensure they are aware of the new rights, including your own staff. Remember too that it is already a general principle of data protection law that personal data should be accurate, where necessary kept updated and not held for longer than necessary.

GDPR 2018 WHAT YOU NEED TO KNOW

PRACTICAL STEPS

Key changes in the GDPR	+ Actions to take now
Direct obligations on processors Under current law, the controller is solely responsible to data subjects and the ICO for compliance. By contrast, the GDPR imposes direct obligations on processors, such as to take security measures to protect personal data and maintain records of all processing activities. Processors won't be able to subcontract processing without the controller's prior consent. The ICO can impose fines on a processor where these obligations are breached.	Map out all your arrangements with data processors, such as outsourced services and cloud suppliers, for example firms that manage your email marketing as well as any IT service providers. Where necessary seek to renegotiate terms to comply with the new law. While this is unlikely for most auctioneers and dealers, check whether your organisation is acting as a processor on behalf of anyone else. If so, you will need to comply with the direct obligations under the GDPR. This could have significant implications for groups of companies which provide services to each other.
New(-ish) rules on data transfers The current law restricts transfers of personal data outside the European Economic Area. The GDPR repeats much of the existing law here and in some circumstances narrows the scope for organisations to legitimately transfer personal information outside of Europe.	Take stock of your data export activities. You will be exporting personal data if a third party stores or processes your customer data or HR data in the US, for example. While the GDPR does not offer any easy solutions, it is important to understand your level of risk and ensure that each of your export arrangements has a legitimate basis.
Overseas rules and regulators Where organisations offer services in more than one EU member state, they will be subject to regulatory enforcement from data protection supervisory authorities in other jurisdictions where customers are located. Note that the GDPR also applies to businesses outside the EU who process personal data of people in the EU. This relates to where the processing relates to the offering of goods or services to them or monitoring their behaviour within the EU (for example, online tracking for the purpose of advertising).	While most dealers and auctioneers restrict their operations to the UK, some will be operating more widely. If so, the lead supervisory authority will be the regulator in the country where you have your 'main establishment'. Consider where this is and identify the lead authority. Keep a close eye out for guidance issued by your lead authority (which will be the ICO for organisations with their main establishment in the UK).

GDPR 2018: Your questions answered

For part 2 of *ATG*'s guide to the General Data Protection Regulation 2018, we have invited readers – auctioneers, dealers and collectors – to pose practical questions to legal and marketing experts.

See pages 10-15 for their answers to these queries.

The Data Controller

THE ANTIQUES DEALERS FAIR

As a fair organiser, The Antiques Dealers Fair Limited hold both business and consumer data. Owners Åke and Ingrid Nilson explain their new responsibilities

"We all tend to go ballistic when new regulations come in, but most of the GDPR rules are based on common sense. They are written with a view to prevent malpractice among list brokers and third party advertisers and, by and large, these are not the people we deal with as fair organisers."

Ahead of changes in May, Kent-based Ingrid Nilson of The Antiques Dealers Fair Limited (TADFL) is taking her company's role as a Data Controller seriously but in her stride. She is doubtless correct when she says that "good practice now will not be so much different than good practice in the future".

Like most fair organisers, TADFL holds two types of customer data – those of exhibitors and suppliers (business data) and those of fair visitors (consumer data). The latter, stored electronically in a format accessible only by Nilson and her husband and business partner Åke, comprises the home and/or email addresses of several thousand members of the public who have expressed an interest in receiving information about the firm's boutique fairs.

"We invite them to fill out a form when they come to a fair," Nilson says. "They may have responded to an advert, received a free ticket from a lifestyle magazine or registered via our website. But if they are our customers' clients we don't assume we can contact them."

In short, TADFL's customers have opted-in to receive marketing material. "We need to prove at least one of GDPR's criteria for holding customer data (see 'GDPR at a glance,' page III). As a general rule it won't be difficult for fair organisers to do that. You would need to be very careful when buying and direct-mailing a third-party list of potential contacts but it's not something that we do."

WEBSITE SECURITY

The primary change for TADFL will be the rebuilding of its website and a focus on website security in particular. Data protected by GDPR includes Internet Protocol (IP) addresses, in other words the fingerprint left by visitors to a website counts as personal data.

It is not just GDPR that has brought this issue to the fore: Google has started prioritising sites using recognised secure systems. The more secure the site, the higher up Google's indexing it is likely to appear.

It helps that Åke Nilson is an IT specialist: "I have already had to read up on GDPR for my other clients," he says.

New privacy statements will also be written and a page introduced to the firm's website where people can ask to be removed from the list.

Similar information will appear at the bottom of marketing emails, whether one of the firm's newsletters or free invitations to area-specific events. Like many art market firms, TADFL uses email marketing system MailChimp. Under the GDPR regime, "we now have to be explicit with customers that MailChimp will be processing our mailings", Åke says.

> We invite visitors to fill out a form when they come to a fair. But if they are our customers' clients we don't assume we can contact them

Data Controller, The Antiques Dealers Fair Limited

Photo by Frances Allitt

The Data Protection Officer

POPPY WALKER

Director, Head of Operations, Forum Auctions

Courtesy of Forum Auctions

Launched in 2016, Forum Auctions was a business built with GDPR in mind. As the May deadline approaches, Poppy Walker discusses her role as the firm's 'DPO'

"Frankly, a lot of the high-level do's and don'ts are largely common sense. My litmus test has always been, if I feel uncomfortable defending an action, then that's a good indication it's sailing too close to the wind."

So speaks Poppy Walker, head of operations at books and works on paper specialist Forum Auctions and the firm's Data Protection Officer, tasked with ensuring the organisation is compliant with GDPR. "I chose the title of DPO to highlight our commitment to data protection compliance," she says. "However, I'm aware that the GDPR doesn't require all businesses to have one (see page 6 – 'Appointing a Data Protection Officer'), so we may change the title once the law comes into force."

Like many seasoned marketers she has long been familiar with the legislation governing the collection, use and storage of data. Familiarity with GDPR's new demands has come via a recent seminar held by auctioneer body SoFAA and the ICO (Information Commissioner's Office) website – see ico.org.uk – which she describes as "a must-read and the main resource for anyone taking on the role of DPO".

GDPR ON THE HORIZON

Forum considers itself to be in a fortunate position. A young business (launched less that two years ago), its systems were designed with GDPR on the horizon.

As such, modifications to systems and protocols will be small. "We ensured we collect data of our buyers and sellers in a secure way and retain only basic contact information – we don't store more personal details and we regularly test our firewall security."

Forum has one main database using Microsoft Dynamics NAV software that allows targeting of clients by interest category. Some clients have niche subject interest areas and only wish to be informed when upcoming lots are relevant.

"We do regularly ask clients to update us on their areas of interest, and use this along with past sales data to select who may be interested in forthcoming items. While it shouldn't breed a sense of complacency, auctioneers and dealers are relatively fortunate in that our industry tends to attract clients who are genuinely interested in the products we offer. In the main, they welcome periodic updates."

Walker believes the most likely source of a privacy complaint would arise from a firm over-communicating with clients. "Across our database, I focus on the extent to which a client has previously engaged with us, the regularity of the engagement and date of last engagement. If the client is a 'trader' or recent 'opt-in' then I see no tangible risk to 'unsolicited' communication. But, trade or private, we allow all email respondents to unsubscribe at any time."

> Auctioneers and dealers are fortunate in that art market clients tend to welcome periodic updates

The relative youth of the Forum database doubtless puts the firm in an easier position to many others. However, the principles and procedure are much the same.

At board level, Forum is currently reviewing all its data collection, storage and deletion processes ahead of the new legislation and agreeing the level of compliance appropriate for a company of its size.

A staff training programme for all employees will follow and, by May, a Data Protection Policy detailing commitments will be available for download from the company's website.

What will a typical week as a DPO look like? Walker says there will be an ongoing need – perhaps on a weekly basis – to monitor data collection and record keeping to ensure contact lists for marketing purposes are relevant, accurate and clients have opted-in to receive communications.

In addition, Walker will "need to be prepared to identify and report any breaches and be the main point of contact for anyone seeking information on our data storage".

The plan is for a first data audit during 2018 and thereafter once every 18 to 24 months – although that could change as clarity emerges around some of the more opaque aspects of the law.

"I believe it is fair to say that no-one yet has a clear insight into what the impact of GDPR will be two or three years hence," says Walker. "The new legislation clearly sets out a very onerous standard when read literally. It might need a number of test cases to pass through the courts to set a series of precedents."

GDPR

Question time: your queries answered

Dealers, auctioneers and collectors ask our experts what the GDPR means for them

Earlier, we introduced the core principles of the General Data Protection Regulation (GDPR) which, when it becomes law on May 25, will change the way businesses must handle the personal data of individuals in the EU. These may seem straightforward – essentially, consumers will have more control over how organisations use their data and there is more responsibility on firms to manage data, with bigger fines for misuse.

But what are the day-to-day realities of the GDPR for art market businesses? We asked readers – dealers, auctioneers and collectors – to submit their queries. Here, data protection legal expert, Farrer & Co partner **Ian De Freitas**, and database marketing specialist **Charles Ping**, chairman of Fuel Data, answer those questions.

Legal eagle:
IAN DE FREITAS,
Partner, Farrer & Co

Ian is a litigator at Farrer & Co with over 25 years' experience, in particular around the areas of IP, technology and data. He is also an expert on data protection compliance and has been helping clients prepare for the changes being brought in by the GDPR in May 2018. Much of Ian's work has a cross-border element. He has strong connections with clients and independent law firms across the world, particularly in the US and Continental Europe. Last year Ian presented on the GDPR to members of auctioneer trade body SOFAA.
farrer.co.uk

Marketing expert:
CHARLES PING
Chairman, Fuel Data, part of Engine Group plc

Charles has over 30 years' experience working with data in a marketing context. He was head of CRM at Guardian Media Group, chairman of the Direct Marketing Association and is an industry commissioner at The Direct Marketing Commission. His role at Fuel includes helping clients to succeed in marketing while meeting the GDPR's requirements.
fueldata.co.uk

> GDPR is designed primarily to protect consumers or in the art market world, private buyers and sellers
>
> **Ian De Freitas,** Farrer & Co

DEFINITION OF 'PERSONAL DATA'

Q1 We are a small auction house running bi-monthly sales and would like to know what exactly is 'personal data'? For example, if we communicate with a buyer via their work email, a dealer perhaps, does that count as personal data?

A Ian De Freitas replies: Personal data is any information about a living individual who can be identified from that data or other information which is reasonably available. It is a very wide definition. It includes an individual's work details, for instance a dealer's email address at his or her place of work.

Remember that at the end of the day, GDPR is designed primarily to protect consumers or in the art market world, private buyers and sellers, though it will still impact business-to-business transactions such as an auction house selling to a dealer.

Charles Ping replies: The basic rule is that if data such as an email address features an identifiable name, for example 'bob.smith@xxx' then it is personal data, but if it's info@xxx, it is not. The easiest route is for you to treat all data, identifiable or not, in the same way.

Picture courtesy of W&H Peacock

PERMISSION TO PROCESS DATA

Q2 On what basis may I process a buyer's or seller's data?

A The Information Commissioner's Office website says: Under the GDPR you need a lawful basis to process data.

There are six available lawful bases – see below – and no single basis is 'better' or more important than the others. Which basis is most appropriate to use will depend on your purpose and relationship with the individual.

Most lawful bases require that your processing of someone's data is 'necessary'.

- **Consent** of the individual whose data you hold (see Q4);
- **Contractual**, where an individual has entered into a contract with a business, for example buying at auction or from a dealer;
- **Legal obligation**, if you need to process data to comply with a law or statute;
- **Legitimate interests**, which can include your firm's own commercial interests, balanced against the individual's interests and rights. The GDPR states that using personal data for direct marketing purposes can be a legitimate interest;
- **Vital interests**, where you need to process data to protect someone's life;
- **Public tasks**, where processing is necessary for performing a task that is in the public interest.

Q3 Under GDPR, customer and potential customer data that I keep in my database must be 'adequate and relevant'. What does this mean in practice for my gallery?

A Ian De Freitas replies: It means that if you have identified 'legitimate interests' as your basis for processing personal data (see Q2), as many businesses are doing, you have a legitimate reason or purpose to keep that customer's or potential customer's data on your database. This might be, for example, for marketing purposes.

Note that tax reporting is a different ground for processing, based on compliance with laws and regulations.

However, if you're relying on legitimate interests, you should keep only what is necessary to achieve that purpose and nothing more. 'Legitimate interests' under GDPR does not entitle you to keep everything, such as a buyer's credit card details or where an item was shipped to.

But it might be legitimate to keep a record of the type of antiques or artwork a customer is interested in by keeping a record of their past inquiries or purchases, so that you can then contact them if a similar item becomes available.

Tell people why you want their data and what they'll get as a result

Charles Ping,
Fuel Data, part of Engine Group plc

CONSENT

Q4 What does 'valid consent' mean under GDPR?

A Ian De Freitas replies: Consent under GDPR is one of the six lawful bases for processing a person's data (see Q2). It means that an individual has given their permission for their data to be processed and this must be (i) freely given (ii) specific (iii) informed and (iv) unambiguously indicated.

In simple terms, if you want to use consent as a basis for processing data then this consent does have to be opt-in (for example, the recipient ticking the box to say 'yes').

However, GDPR accepts that the necessary clear, affirmative action can be indicated by other means.

For example, you could obtain consent from a customer in the middle of a transaction in the following way. Having explained to the customer that, for example, you want to market to them in a certain way, you then give them the option to proceed with marketing in that way, or an equally prominent box which says that they don't. The customer's choice is then recorded in that way and the particular online transaction continues.

This illustrates another point. For consent to be valid, it has to be 'informed consent' – in other words, a very clear explanation has to have been provided to the customer about what will be done with their data and they have agreed to this.

If you can demonstrate that you showed what you will do with that data – for example, mailing them a physical catalogue – it can be valid for a long period of time if nothing changes.

However, consent is unlikely to be indefinite. In reality, you are likely to need to re-permission your database on a reasonably regular basis, but this is bound to happen organically if you are complying with GDPR.

Charles Ping replies: Consent must be informed, freely given, not bundled with other services and as easy to withdraw as to give. This is not complicated to do:
- Tell people why you want their data and what they'll get as a result;
- Have a clear tick box or statement that says: 'Give us your email address and we'll send you details of all forthcoming auctions and sales';
- Have a clear unsubscribe process and make sure it works;
- Anyone who hasn't opened an email in the past 12 months should get a 'Do you still want to hear from us email?' and if there is still no response, delete them from your database.

If someone buys something at your auction house, gallery or antiques shop, you have the right to process their personal data to complete the sale. However, that alone doesn't give you the right to market again to that person. That would be covered by either consent (Q4) or the legitimate interest of the dealer or auctioneer business to market themselves (Q3).

However, take care of the law governing electronic communications, known as PECR (see Q8, below).

Q5 Within the bounds of GDPR, how can I legally encourage customers to consent to my dealership processing their data?

A Ian De Freitas replies: GDPR does not like the idea of people 'selling' their data for a benefit. With that in mind, consent cannot be related to incentives and you should not attach conditions to customers giving their consent.

You can point out to customers the benefits of staying in touch, for example that it means you can give them timely information about forthcoming sales or lots. Overall you could underline the fact that if they object to you using their data to communicate with them, then you can't stay in touch with them.

RIGHT TO BE FORGOTTEN

Q6 I'm a dealer and need to know what is GDPR's impact on records that are required to be kept for VAT purposes, such as hard copy or electronic invoices which contain customers' contact details and may also have other information about them?

A Ian De Freitas replies: The GDPR 'right to be forgotten' (or erasure) principle is not absolute. If your firm has a need, such as a legal or regulatory requirement, to keep some of the data, then it can do so. However, it can only keep and use that data for that purpose and no other. And it must delete the data once any time-limit for its retention is exhausted.

MARKETING

Q7 Should I be contacting my customers now to get them to opt-in to marketing from May 2018?

A Ian de Freitas replies: You should be contacting customers now, seeking the right to continue to process and use their data.

Be careful if you're using electronic channels, such as email, to contact customers for this purpose – see Q8.

Your customers don't necessarily have to opt-in to marketing. Under GDPR, you could rely on another ground to process their data for marketing purposes, which is called 'legitimate interests'.

To rely on this aspect of GDPR, you have to balance your legitimate interest in marketing to those individuals against their rights not to be contacted if they don't want this, or contacted in a way which is annoying (for example, spamming customers with multiple communications) or intrusive. So, you have to assess the position carefully (and keep a record that you have done this).

If you decide that you do think you can rely on the 'legitimate interests' test, then you have to be transparent about that and tell your customers that this is your basis for marketing to them and if they want to object then they can do so.

Q8 Can I continue to send marketing emails to my current database?

A Ian De Freitas replies: Email marketing is additionally governed by a different piece of EU legislation designed (partly) to deal with direct electronic marketing (for example, via emails and texts). This EU legislation is known in the UK as the Privacy and Electronic Communications Regulations or PECR.

All businesses have to comply with PECR. It stipulates that you can only send direct unsolicited marketing by electronic means to individuals where you have their prior consent. The one exception to this, however, is the so-called soft opt-in rule.

This says that you can send unsolicited electronic marketing communications without consent if:
1. You obtained the recipient's contact details in the course of a sale or negotiations for a sale to them;
2. At that time, you gave recipients an easy means to refuse to receive marketing in this way and you offer that easy means to refuse marketing on each subsequent occasion that you send such messages to them;
3. You are marketing similar goods or services to them to those originally offered.

These PECR rules are also being revised by the EU but for the moment, you should continue to comply with the current PECR rules.

Charles Ping replies: Those people who are neither opening nor reading the emails are of questionable digital marketing value to your business. If people are still opening and reading your emails, you will have a much easier time converting their consent.

Q9 My auction house would like to use email to tell customers how we want to use their data. Is this allowed under GDPR?

A Ian De Freitas replies: There is an added complication if you communicate this by email or by text and you are explaining how you want to market to customers. The view of the UK data protection regulator is that this is a marketing communication which is governed by PECR.

If you do not have prior consent to send such communications or you cannot rely on soft opt-in, then you are at risk of being in breach of PECR (see moneysupermarket.com case study, page 14).

You could instead contact the customers by post or give them the necessary information next time they visit your gallery or auction house. This doesn't fall foul of PECR.

Charles Ping replies: With email and catalogue content being served online, the best way would be to have a really frank pop-up box on your home page simply explaining that if the person wants to receive emailed sales details, can they please agree to this revised statement.

Q10 I'm a collector who bought once from a particular auction house. They now send me text messages about forthcoming sales and I don't recall giving them my permission to do so. Will this be legal under GDPR?

A Ian De Freitas replies: Under GDPR, the auction house would have to have a lawful basis to send you these text messages. That lawful basis could either be that they obtained your consent or they are relying on their legitimate interests.

If they are relying on consent and it was obtained in an opt-out way, then that will not be good enough once GDPR takes effect. If they are relying on legitimate interests they will need to show that they explained this to you at the time.

In addition, because these are text messages then PECR comes into play. As explained above, to send electronic marketing communications like this, the auction house will have needed to have your consent or have set up the soft opt-in exception referred to previously.

Q11 I'm a dealer who exhibits at fairs and use these occasions to collect customer and prospect details for marketing purposes. I want to continue doing this, but will I be breaking the new law?

A Ian De Freitas replies: This is a good example of where GDPR and PECR intersect.

For GDPR purposes, to be allowed to collect and use the data for marketing purposes, you would have to explain to customers and prospects that this is what you are doing, what you propose to market to them and how you will communicate with them. GDPR says that you should be explaining all of this at the time you collect the data from these individuals and the best and clearest way to do this is to provide them with a Privacy Notice setting it out.

> The GDPR states that using personal data for direct marketing can be a legitimate interest
> **Information Commissioner's Office**

> Under GDPR an auction house needs a lawful basis for sending you text messages
>
> **Ian De Freitas**

For PECR purposes, you have to remember the special extra rules that apply if you want to contact these customers for marketing purposes via electronic means. If you want to do this, then you either have to obtain their consent or set up the soft opt-in arrangement described in Q8.

However, the problem with soft opt-in is that it seems difficult to argue that the contact details of the individual were obtained in the course of a sale or negotiations for a sale to them, when all that they might be doing is just attending a fair.

So, the safe option is to obtain their consent.

Charles Ping replies: I doubt that simple collection of data at a fair could be called 'negotiations for a sale' which is the language used in relation to soft opt-in in PECR. However, consent does not have to be a tick box. The line 'give us your email address and we'll send you details of all forthcoming auctions and sales' is consent and lawful, as long as you are not bundling that up with something else like a giveaway or a competition.

Q12 In what way will we legally be able to undertake database building using bought-in lists for marketing purposes after May 2018?

A Ian De Freitas replies: Buying in data from third parties will be very risky after May 2018. It is likely that third parties will not have had the necessary GDPR compliant permissions from the customers to pass their data to you. You should thoroughly test this before buying in the data.

Once you buy it in then you should tell the customers that you now have their data and explain to them what you intend to do with it by sending them a fully compliant GDPR notice. You must do this within a maximum of one month of acquiring the data. If they reply objecting to this, then you must stop marketing to them.

FRAUD DETECTION

Q13 Can I continue to use customer data to report suspicious activity such as suspected fraud to authorities?

A Ian De Freitas replies: Yes. GDPR recognises that there are lawful bases to use personal data in this way, as outlined in Q6.

BREACHES OF GDPR

Q14 An employee left our firm and, it seems, took a copy of our customer database with them. What does GDPR say about such incidences?

A Ian De Freitas replies: This is a breach of GDPR by the ex-employee and by their new firm. Both are exposed to the sanctions regime in GDPR.

After May 25, such breaches must be reported to the ICO within 72 hours.

PRIVACY NOTICES

Q15 Is there an example of a GDPR privacy notice I can consult?

A Ian De Freitas replies: There are guidelines on the ICO website (ico.org.uk) on the transparency and consent points your policy needs to cover – put the words 'ICO consent guidance checklist' into a search engine to take you there.

You'll also find the GDPR privacy policy guidelines published in December 2017 by the Article 29 Working Party (a body of EU data protection regulators) helpful,

SHOWING COMPLIANCE

Q16 We're supposed to be able to demonstrate compliance with GDPR, if the authorities ask us to. How can we do this?

A Ian De Freitas replies: This is the concept of 'accountability', something the ICO is very keen to push. Ideally, you should have a document which sets out that

CASE STUDY: Moneysupermarket.com gets fined

In 2017 the Information Commissioner's Officer (ICO) sent a strong message to businesses that it will penalise them for breaches of data privacy law.

What happened?

Price comparison website Moneysupermarket.com sent more than seven million emails asking people on its database to reconsider their previous decision to opt out of receiving direct marketing messages.

What did the email say?

It included a section entitled 'Preference Centre Update' which read: "You've told us in the past you prefer not to receive [promotional email]. If you'd like to reconsider, simply click the following link to start receiving our emails."

ICO response:

Moneysupermarket.com was fined £80,000 by the ICO for ignoring customers' email stated preference to opt-out. "Emails sent by companies to consumers under the guise of 'customer service', checking or seeking their consent, is a circumvention of the rules," the ICO said.

Response from Moneysupermarket.com:

The firm apologised "unreservedly" for "this isolated incident," adding that it had "put measures in place to ensure it doesn't happen again".

ICO issues £80,000 fine

you considered how the GDPR affects your business, what you decided to do to address the issues raised and how you then went about ensuring the necessary steps were taken. This should be regularly reviewed.

In particular, if you are making changes which affect the processing of personal data then you need to document that you thought about this and what you did to address any issues. This is sometimes called 'Privacy by Design'. You should add this assessment to your overall compliance record.

In terms of keeping particular types of records, yes, you should keep records of consent where this has been given. For customers, that record could sit with the data that you are keeping about them which they have consented to.

LAPSED CUSTOMERS

Q17 How long may I keep the data of lapsed bidders/customers? What does 'lapsed' actually mean under GDPR?

A Ian De Freitas replies: There are several reasons to keep data of individuals after your relationship with them has ended. For example, you might need to keep the records of particular transactions with them because of the possibility of legal claims or regulatory reasons (for example, to comply with money laundering regulations).

For transactional records, a reasonable period would be six years after the transaction concluded (this is the normal limitation period for bringing breach of contract claims). Again, to comply with GDPR's Accountability clause, keep a record of how you arrived at the retention periods. This is sometimes called a 'Data Retention Schedule'.

You need to place this lapsed customer data in a separate storage area on your database so that it can't be used for anything else.

PROCESSING DATA OUTSIDE THE EU

Q18 We're a US-based dealer with many clients located in EU countries. Does GDPR apply to how we manage this data?

A Ian De Freitas replies: Yes, it does. This is because the GDPR is extending the reach of EU data protection laws to businesses based outside the EU who are processing the personal data of individuals located in EU countries, in the context of offering goods or services in the EU to those individuals.

This is sometimes referred to as 'pay to play' – ie, if you want to market to customers in the EU, then you have to abide by EU rules.

ANTIQUES TRADE gazette
THE ART MARKET WEEKLY

EXCLUSIVE SUBSCRIPTION OFFER

Your first 12 issues for just £12

– that's only £1 per issue

YOUR SUBSCRIPTION INCLUDES:

- ✓ **Your first 12 issues for just £12 – that's only £1 per issue**
- ✓ Weekly delivery of the newspaper
- ✓ Unlimited access to antiquestradegazette.com
- ✓ Antiques Trade Gazette mobile and tablet app
- ✓ Editor's newsletter with a pick of the top stories
- ✓ Antiques Trade Gazette online archive going back to January 2017

Whether you buy, sell or merely observe and enjoy the art, antiques and vintage markets, Antiques Trade Gazette is the must-read newspaper. Every issue is packed with breaking news, exclusive information and market intelligence to ensure you are always one step ahead.

Noelle McElhatton *Editor, Antiques Trade Gazette*

To place your order call us now on +44 (0)20 3725 5507 or complete the form below:

Place it in an envelope and mail it FREE of charge to: Antiques Trade Gazette
Freepost RTHX-RYZY-YUHA,
The Harlequin Building, 65 Southwark Street, London SE1 0HR

☐ Yes, I would like to subscribe to Antiques Trade Gazette and get my first 12 issues for £12 by Direct Debit. Saving 75% (then £24.75 a quarter thereafter saving 50% annually).

MY DETAILS

Title First name

Surname

Address

Postcode

Tel number

Email

Your personal information will be used as set out in our Privacy Policy, which can be viewed at **antiquestradegazette.com/privacy-policy**

OTHER PAYMENTS - for an annual print & digital subscription

☐ UK - **£129** ☐ Outside the UK - **£168**

I enclose a cheque made payable to Auction Technology Group for £

☐ Visa/Debit card ☐ Mastercard ☐ American Express ☐ Maestro

Card number ☐☐☐☐-☐☐☐☐-☐☐☐☐-☐☐☐☐

Expiry Date ☐☐-☐☐ Security Code ☐☐☐☐

Signature Date

Offer ends 24th February 2018.

Instructions to your bank or building society to pay by Direct Debit

DIRECT Debit

Name of bank

Address

Postcode

Name(s) of account holder(s)

Bank/building society account number ☐☐☐☐☐☐☐☐

Branch sort code ☐☐ ☐☐ ☐☐

Service user number: 1 6 9 1 3 7

Please pay Metropress Ltd Direct Debits from the account detailed in this Instruction subject to the safeguards assured by the Direct Debit Guarantee. I understand that this Instruction may remain with Metropress Ltd and, if so, details will be passed electronically to my bank/building society.

Service user name: Metropress Ltd

Registered address: The Harlequin Building, 65 Southwark Street, London SE1 OHR, UK

Reference number (internal use only)

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Signature Date

Banks and building societies may not accept Direct Debit mandates from some types of account.

DIRECT Debit

The Direct Debit Guarantee

- This Guarantee is offered by all banks and building societies that accept instructions to pay Direct Debits.
- If there are any changes to the amount, date or frequency of your Direct Debit, Metropress Ltd will notify you 10 working days in advance of your account being debited or as otherwise agreed. If you request Metropress Ltd to collect a payment, confirmation of the amount and date will be given to you at the time of the request.
- If an error is made in the payment of your Direct Debit, by Metropress Ltd or your bank or building society, you are entitled to a full and immediate refund of the amount paid from your bank or building society – If you receive a refund you are not entitled to, you must pay it back when Metropress Ltd asks you to.
- You can cancel a Direct Debit at any time by simply contacting your bank or building society. Written confirmation may be required. Please also notify us.

Notes

ANTIQUES TRADE gazette