nucleus

GDPR – a guide for financial advisers

Nucleus white paper

Edition 01

Date of publication 14/3/2018

Prepared in partnership with Phil Young, Zero Support

Contents

1. Introduction

Advisers are all too aware that the next wave of regulatory reform is never far away. While the aftershocks of MiFID II are still being felt, advisers are having to contend with the next set of rule changes looming on the horizon: the General Data Protection Regulation, or GDPR for short.

Nucleus has compiled this white paper, together with Phil Young of Zero Support, to help advisers make sense of the requirements and how they apply to their business. It draws on a lot of the useful guidance that exists already, particularly from the Information Commissioner's Office (ICO), but drills down deeper to explain how the regulation will apply on a practical level to advice firms and financial planners.

We have provided some context as to how GDPR extends the existing rules on data protection, and set out what advisers need to consider when they are processing data for both clients and staff. We have packed in lots of practical examples, including the GDPR implications for buying a client bank and what to consider on client newsletters, as well as key takeaways, action plans and checklists so that you can benchmark your progress.

Some advisers may be quite far down the road on getting their business GDPR-ready, while others may be just starting out. We hope this white paper both reassures those who have already begun their GDPR preparations, and also helps with making the job of GDPR compliance a little less daunting.

Natalie Holt
Content editor, Nucleus

2. Background

The General Data Protection Regulation (GDPR) will come into force on 25 May 2018. This is an EU regulation, which applies instantly without the need for UK interpretation or legislation, unlike an EU directive. It will be enforced in the UK by the Information Commissioner's Office (ICO).

There are other rules to consider alongside GDPR. In particular, the ePrivacy Regulations will replace the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) from 25 May 2018. These regulations contain additional rules for electronic marketing (including email, telephone, cookies, SMS and social media) which often go beyond the GDPR.

This guide covers both the proposed ePrivacy Regulations and GDPR. In summary, the GDPR will apply if you are processing data. If you are simply marketing without any data processing then you can just refer to the ePrivacy Regulations.

IT, network and physical security issues are huge topics in their own right so haven't been focused on here. The rules emphasise data security should be appropriate and adequate, so it's up to individual firms to decide what is adequate for their business based on the data they hold, how it is processed and industry standards. Advisers will also need to consider the relevant advertising and promotion rules from the FCA, the Advertising Standards Authority and other regulatory bodies.

The ICO website gives a lot of useful and practical information about the GDPR and how it should be implemented, although further clarification can be expected throughout the year. You can complete their quick checklist on GDPR along with wider data protection toolkits, and read their high level guide 'Preparing for the General Data Protection Regulation (GDPR) – 12 steps to take now', on their website ico.org.uk.

While many of the principles of the GDPR reflect the UK's Data Protection Act 1998, there are some new rules to consider.

These include:

- The right to 'be forgotten' and the right to have data transferred to another business.
- Tougher disclosure requirements on privacy policies and when obtaining consent to process personal data.
- The right be informed if there has been a personal data breach likely to result in a high risk to the rights and freedoms of individuals.
- Fines of up to 4 per cent of turnover or €20m, whichever is greater, for businesses caught breaching the rules.

2.1 Why do we need protecting?

It's easy to assume GDPR is just about protecting people from unsolicited marketing and guarding against identity theft. But it's far broader than that. Big data is big business. There are companies collecting, storing and using vast amounts of highly personal data about every aspect of our lives.

The way Facebook groups and segments its users provides a powerful set of advertising tools with which to target its 2 billion users. This example alone shows how times have moved on since the Data Protection Act.

We now know some airlines manipulate the price of flights based on how often you visit their page. The cookie they store in your browser tells them to increase the price each time you visit the page to pressure you into buying. Clear your cookies in your browser settings and the price will drop down again (see the Cookies and Consent section for more information).

Researchers in Spain found that when shopping with artificially created online profiles, prices varied depending on the wealth of the person shopping. The wealthiest online shoppers were offered the same set of headphones at around four times the price of the least wealthy. Airline tickets varied by 166 per cent. This is personalised pricing by stealth.

Experian, which holds data on 44 million UK citizens, was hacked in 2015, bringing international attention to the scale of security breaches. But protecting data has always been a key aspect of regulation. The ways in which data is processed, particularly profiling and targeting for sales and marketing purposes, has radically changed since the growth of the internet in the mid 1990s. The GDPR, and the new ePrivacy Regulations, attempt to acknowledge those changes.

2. Background

2.2 Brexit

Brexit is unlikely to have a significant impact on GDPR. UK data protection rules are due an overhaul anyway, and not adopting regulations equivalent to GDPR means the European Commission could reject the UK's application for 'adequacy' status. This is required to allow the free flow of information between the UK and EU without the need for separate contractual arrangements. So, while GDPR could be amended or watered down post-Brexit, it's best to assume this will not happen in any material way. The UK's own data protection bill clearly indicates a UK intention to replicate GDPR post-Brexit.

To illustrate the point, the implications of GDPR for US companies who collect, maintain or process personal data of EU citizens has already been recognised. PwC has reported significant investment in this area by large US businesses who are already compliant with the EU-US Privacy Shield, due to the GDPR's broader scope.

2.3 SMEs and special category data

Businesses with under 250 staff have reduced obligations under the GDPR when it comes to formally documenting processes and carrying out a data protection impact assessment. However, these exemptions do not apply to processes which are higher risk, including those where 'special category' data is processed. Special category data includes somebody's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. It also covers the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, or data concerning health, a person's sex life or sexual orientation.

Due to the nature of the information required to give financial advice, it is inevitable that both staff (including self-employed advisers or other control functions) records and client records will include special category data. Even a profile picture on a customer relationship management system (CRM) or intranet could be 'biometric data for the purpose of uniquely identifying a person'.

Processing special category data is only permitted in a very narrow range of circumstances. Those most applicable to an advice firm are where explicit consent is given, or under employment law, emphasising the importance of consent for a financial services business where health information is processed.

2.4 Business to business marketing

The GDPR does not technically apply to business to business marketing as it applies to personal data, however you should be very cautious about using a lower standard for corporate marketing.

Firstly, the legislation treats sole traders and partnerships (but not LLPs) as individuals, so only public or limited companies or LLPs are excluded from the protections offered by GDPR.

Secondly, there is a strong, albeit unresolved, argument that email marketing sent direct to an individual with their own email address (that is, firstname.surname@xyz.co.uk as opposed to a generic sales@xyz.co.uk) is defined as personal rather than business marketing under both the GDPR and the draft ePrivacy Regulations. Already, under section 11 of the Data Protection Act, individual employees have a right to stop any marketing being sent to that type of email address, in other words, an opt out. If individual business email addresses are to be caught under the ePrivacy Regulation that means upfront consent is required, not just an opt out, when marketing electronically.

2.5 What do we mean by personal data?

Personal data is defined as 'any information relating to an identified or identifiable natural person', also know in the jargon as a 'data subject'. An 'identifiable natural person' is someone who can be identified, directly or indirectly, through the data, particularly by name, an identification number or location. It also covers online identifiers specific to a person's 'physical, physiological, genetic, mental, economic, cultural or social identity.'

3. Principles

There are seven high level principles on which GDPR is based, and which inform the specific requirements for processing personal data.

Personal data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency);
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation);
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation);
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay (accuracy);
5. Kept in a form which permits identification of data subjects for no longer than is necessary (storage limitation); and
6. Processed in a manner that ensures appropriate data security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage (integrity and confidentiality).

In addition,

7. The data controller must be responsible for, and be able to demonstrate compliance with all of the above principles (accountability).

3.1 What do we mean by data processing?

Data processing means operations performed on personal data, whether or not through automated means. It includes collecting, recording and organising data, as well as storing it, changing it, retrieving it, and sending it elsewhere. It also covers restricting and destroying data.

3.2 Who are data controllers?

A data controller is a person, public authority, agency or other body which, alone or jointly, decides how and why data will be processed, according to European Union law and the laws of member states.

4. Accountability and governance

The seventh principle, accountability, means there is a need to evidence how you comply with the new regulations. The complexity of this will be far higher for larger firms, but even a small business needs to understand how this should be done and what the consequences are. Much of this will come as no surprise to advisers who are used to regulation.

4.1 Data protection officer

Only big businesses whose activities involve the regular and systematic monitoring of data and public authorities need to formally appoint a designated data protection officer. However, other businesses including your own will still need to designate an individual to take responsibility for data protection compliance, so someone will need to take personal responsibility for this area.

4.2 Reporting breaches

You have to notify data breaches where someone is likely to have suffered damage, for example through identity theft, a breach of confidentiality or financial loss. This is already an obligation under the Data Protection Act, yet the increased fines under GDPR and the growing reputational damage in this area will generate more notifications.

You need to notify the ICO within 72 hours of becoming aware of the breach. You must also notify the people concerned as soon as possible if the breach is likely to result in a high risk to their rights and freedoms. This is a slightly higher threshold than for notifying the ICO.

Given the risk of identity theft and financial crime within advice firms due to the detailed nature of the information held about clients and their policy details, you may wish to produce a standard process and wording that clients can follow if their data is stolen, including changing passwords and notifying platforms, life companies and fund groups in order to reduce the risk of their data being used fraudulently.

For example, a notification to clients might include:

- What has happened and whether the event appears to specifically target client data or if this was incidental.
- What the possible consequences to the client are, for example, identity theft, fraudulent withdrawal of money.
- What steps you have taken, such as notifying the ICO, the police, platforms, life companies and fund groups, with a temporary block on any withdrawals of cash or changes to personal details.
- What steps the client can take such as notifying their bank and other financial services firms.
- Clients may want to change their passwords – the advice here is to use strong passwords and two-factor security if available.
- Clients should check future post for any suspicious activity such as requests for a change of address.
- They should also consider monitoring accounts on an ongoing basis if identity theft is suspected.

A notification to the ICO must include:

- The nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned; and
  - the categories and approximate number of personal data records concerned
- The name and contact details of the contact point for data protection.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

4. Accountability and governance

4.3 Fines

These new rules are meant to be taken seriously, as demonstrated by the heavy fines in place for non-compliance. The new fine cap is the greater of €20m or 4 per cent of annual global turnover for serious violations, or €10m or 2 per cent of turnover for lesser violations. This is a huge increase from the £500,000 maximum fine under the Data Protection Act.

The punitive maximum fine has certainly grabbed the attention of large businesses, as well as consultancy firms spotting an opportunity to charge high fees. The challenge, even for smaller businesses, is raising standards and public awareness together means complaints about breaches, both spurious and legitimate, are bound to increase.

Things to consider

- Who in your business takes responsibility for data protection and complying with the GDPR?
- Where data breaches occur, make sure you notify the Information Commissioner's Office within 72 hours of the breach
- Do you have a process for clients to follow if their data is stolen?

The increase in ICO penalties pre-GDPR

Year	Number of fines	Total amount of fines
2010	2	£160,000
2011	7	£541,100
2012	17	£2,143,000
2013	14	£1,520,000
2014	9	£668,500
2015	18	£2,031,520
2016	21	£2,155,500
2017	51	£3,961,500

5. The six lawful bases for processing data

Under GDPR, data can only be processed under one of six lawful bases. A different basis may apply to different types of data or how it is processed, but you must be certain which one of these apply.

1. Consent
2. Legitimate interest pursued by a controller
3. Necessity for fulfilment of contract
4. Legal obligation
5. Necessary for vital interests of the data subject
6. Necessity for performance of a task in the public interest

The first three, and on occasions the fourth basis, are the most relevant for advisers. Consent is the most obvious first choice, but not always easy to obtain.

5.1 Consent

> "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.
>
> This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data.
>
> Silence, pre-ticked boxes or inactivity should not therefore constitute consent.
>
> Consent should cover all processing activities carried out for the same purpose or purposes.
>
> When the processing has multiple purposes, consent should be given for all of them.
>
> If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."
>
> The General Data Protection Regulation

Consider how many people you've added to a mailing list for a newsletter or bulk email. How many specifically and positively consented to being added to that list?

Depending on the situation, consent is not always easy to obtain. It should be relatively easy when signing up a new client. But consent to be marketed to, for example, will be harder under GDPR and ePrivacy and it can no longer be hidden in terms and conditions. It needs to be obtained separately, prominently and with more detail than ever before, especially if you use data for profiling purposes and not just basic contact details for a generic mailing.

5. The six lawful bases for processing data

Requirements

If you intend to rely on consent, you'll need to keep a record of when consent was obtained, and that the relevant information required by GDPR was provided. The information includes:

- Information about the data controller and contact details of the data protection officer (if one is required).
- What data processing is done and the legal basis for doing it, for example, compliance with a legal obligation.
- Who you'll pass the data to. If you need to define a category of recipients rather than give exact names this should be as specific as possible, so you can't just say "to our select partners".
- How long you'll keep the data.
- If you store or pass data outside the EU, how you'll protect it. This will affect services like Dropbox and MailChimp, and will require you to look into their privacy policies.
- How to request a copy of the data or to have data amended, restricted in use or erased.
- The right to data portability.
- How to withdraw any consent given.
- How to complain to the ICO.
- Any statutory or contractual necessity for the data.
- The existence and significance of any automated profiling or decision-making.

Much of this will be included in your client agreement, but that will only capture consent for clients, not prospects or former clients. A privacy policy can be used to make the standard elements of this information available online or in paper for a variety of purposes.

Importantly, consent cannot be built in as a condition of a service. You must give a clear choice to opt in or not, and the ability to withdraw consent. If you have to process data in a specific way so that it has to be a mandatory part of your service then you should rely on the 'necessity for fulfilment of contract' basis instead.

There is no set expiry date for consent but it cannot be assumed to continue indefinitely. The context must be considered to establish if it is reasonable to still expect contact, so a long period of non-communication since the original consent could render it less reliable.

Profiling and personalised content

It's important to remember there can be several processes which your personal data could be subject to. You may have ticked a box on a shopping website consenting to be sent a marketing email or newsletter promoting products.

But did you also give consent for that same business to store, hold and use other data about you, such as your browsing history, purchases, location or mobile device used? Modern marketing relies on collecting and combining as much personal information about you as possible, so that adverts can be as personalised as possible. That can be useful when recommending music, books or movies you'd love but had never heard of before. But you might also be concerned, given this information can be hacked and stolen like any other, or sold on to other businesses where you don't get the same benefits.

The process of sending a marketing newsletter is separate from the process of profiling data to tailor content and target advertising, and you will need to establish the legal basis for each. They may be different. For example, consent for the newsletter, but legitimate interest for profiling.

For this type of personalised content, should you use it, you will need to:

- Set the expectation when obtaining consent that your content will be tailored and will make recommendations based on their interests.
- Link to the relevant section in your privacy policy which explains how you track data to understand their interests, what you do with it, why, the benefits and their choices.
- Offer a choice between bespoke content based on their interests and non-personalised content. This way, if they currently don't want to be tracked and profiled they can still be an email subscriber – and they can always opt-in to curated, targeted content later.

5. The six lawful bases for processing data

Example

You want potential new customers to sign up to an email newsletter by providing their email address and some basic information via your website. The web form sends a secure email to a member of staff who enters the data onto a spreadsheet stored on your server. The newsletter is sent via an online marketing system where email addresses and names only are stored.

The information you want is:

- Name
- Postcode
- Email address
- Age
- Retired/employed/self-employed

Let's assume the reason you want so much information is you have a number of different specialisms and services within your business (young accumulators, at retirement, long-term care, inheritance tax planning etc) each with their own newsletter content, and you want to send the content which is most likely to appeal to that prospective client. This analysis is a process you undertake on the data, in addition to storing it electronically on your server and in your online email system, and in addition to using it for issuing the newsletter.

You are targeting new prospects rather than clients, so consent is the obvious legal basis for processing this data. This means you need to ask the client to clearly opt in to the service while providing clear information about what that means.

Your opt in box could look like this:

Please tick to opt in to receiving our email newsletter which is personalised for you.

I agree ☐

Opting in means that you are consenting to receive our monthly email newsletter to the address supplied. You have also supplied further personal information about you and you are also providing your consent for us to process this data to profile you so as to provide curated content.

Please tick to opt in to receiving our non-personalised email newsletter.

I agree ☐

Opting in means that you are consenting to receive our monthly email newsletter to the address supplied. It will not be personalised to you, and we will not store any information other than your name and email address.

Whichever option you choose, you can withdraw your consent at any time by emailing phil.young@zerosupport.co.uk and we will stop emails and delete your records. There is an unsubscribe link on every newsletter. We won't pass these details on to third parties for marketing purposes, and all data is looked after in accordance with our Privacy Policy which you can read here.

What you can't do is make this a contact form for an initial enquiry and insist that by submitting the enquiry form the prospect will be automatically added to an email list. This is because consent to the email newsletter cannot be a condition of another service and has to be opted into separately and explicitly.

Nor can the boxes be pre-ticked.

It must be as easy to withdraw consent as to give it, so the provision of an email address in addition to the unsubscribe link within the emails themselves gives the ability to withdraw consent without waiting for another email.

5. The six lawful bases for processing data

Children and consent

Under the GDPR children under 16 cannot give consent for digital services, only the parental guardian can give this, and businesses must use 'reasonable efforts' to verify this consent using digital technology. There is not the same clarity for non-digital services, but attention must still be paid to the clarity and accessibility of information to children in relation to the processing of their data. Advisers will be used to dealing with investments for children (for example, Junior Isas) through parents and grandparents, so it is worth remembering these restrictions.

Cookies and consent

You probably have a warning on your website about cookies. A cookie is a text-only string of information that a website transfers to the cookie file of the browser on your computer's hard disk so that the website can remember who you are each time you visit. They are used to recognise you, organise content, and personalise advertising.

Most cookie warnings obtain consent in a way which technically breach the principle of consent under GDPR as accepting them as a condition of service. If you do not accept them you will not be able to use the website. GDPR and ePrivacy will require browser settings to block cookies by default or provide more configuration assistance with this issue during installation, by 25 May 2018. Already installed systems will have until August 2018 to facilitate this.

This will have an impact on targeted digital advertising such as banner ads and pop-ups, which rely heavily on cookies, as more explicit consent will be required.

It seems unlikely that configuring a browser setting to accept cookies (and other similar technologies) will count as adequate consent for all website cookies alone. However, the days of the current, generic website cookie disclaimer look to be over.

Analytics tracking, which is probably the main thing advisers use a cookie for on their website, is exempt from this, as non-user specific information about website traffic is deemed to be too low risk to cause concern.

The new rules on Wifi-tracking, which allow the location of a device to be monitored as it is carried about, seem surprisingly liberal given their controversy. Tracking is permitted so long as the information is collected to provide a connection and there is suitable notice and an opt-out.

5.2 Legitimate interest pursued by a controller

"The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.

Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.

At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.

The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing."

The General Data Protection Regulation

5. The six lawful bases for processing data

Consent is not always possible. You may have gathered data and information over the years without ever thinking it could be used for marketing purposes at some future date. You have clients who have provided you with huge amounts of personal information which you might now want to use to create a tailored newsletter. Alternatively, you might want to produce a marketing email about a seminar which you know certain clients will be interested in because of advice you've given before. You won't have obtained consent for this previously, as even if you obtained consent to issue a newsletter that doesn't mean you've obtained consent to use their data in such a way that you can profile the right clients to target. However, you may rely on legitimate interest as the legal basis for processing data in this way and issuing marketing material or a newsletter.

Using this as the legal basis will feel less secure than consent, and rightly so. It is open to interpretation and there is likely to be more guidance to follow on this legal basis than any other. However, it is perfectly valid and should be used when appropriate. If you decide to use consent as the legal basis to process data and then fail to obtain that consent, you cannot then revert to legitimate interest as an alternative.

It is also important to note that as far as unsolicited direct marketing is concerned, the GDPR allows legitimate interest to be used as a legal basis for non-electronic direct marketing, such as by post. This does not extend to unsolicited electronic direct marketing, including email, SMS, fax, telephone, and social media. For these types of communication the ePrivacy Regulations will apply. ePrivacy does not allow electronic marketing to be undertaken without consent. So, for unsolicited marketing using an electronic method, legitimate interests is not a valid basis as it will contravene ePrivacy even if it passes the GDPR.

Example

Starting a newsletter about advice and planning issues and sending it to existing financial planning clients is a good example of something that should sit within the legitimate interest definition, provided you have undertaken some additional work to validate this.

Let's look at the criteria required to qualify for this legal basis.

Relevant and appropriate relationship

Clearly, this is far easier to establish for existing clients or someone who has been a client in the past but hasn't been in touch for some years, provided they haven't told you they don't want future communications or have actively terminated the relationship.

Reasonable expectations

If you wanted to market or provide information about a financial service or product which you felt was relevant to your clients, then given the nature of your work it is reasonable for them to expect this. If you marketed a non-financial service or product to them then this is less clear. For example, you might promote a luxury holiday company to your clients. This is non-financial, but you could argue it was reasonable to expect this if you discuss dream holidays with your clients in planning conversations, and explain this in your promotion.

Necessity

A good example of necessity is chasing down unpaid invoices by passing personal information to a third-party debt collection agency. Clearly there is an existing relationship and it is reasonable to expect that an unpaid invoice will result in debt collection. There is necessity to chase down debts for the survival of any business and this would outweigh the rights of the individual. The necessity of a newsletter is less pressing but nonetheless does qualify and there should be no concerns about the impact on the rights of the individual which helps make the case.

If the newsletter is issued by post then the GDPR legitimate business interest legal basis can be used. If the newsletter is electronic then the ePrivacy Regulation applies, but the only addition is to include the ability to opt out of future communications. ePrivacy allows electronic marketing without explicit consent to your clients as there is a clear, established business relationship.

5. The six lawful bases for processing data

If you do rely on legitimate interest then the requirements are less stringent than for consent, but they are still significant. You will need to:

- Provide an opt out to future data processing, ensuring it is "presented clearly and separately from any other information".
- Highlight, while collecting data, any processing which wouldn't be automatically expected.
- Be able to prove the legitimate interests override the interests of the individual.

Any future objection to processing done under a legitimate interest basis must be considered and the burden is on the data controller to demonstrate they have compelling grounds which override the individuals' right to object. However, any objection to future direct marketing is absolute and must be acted on immediately.

It is far safer to rely on legitimate interests, which will always be more open to criticism than consent, where you have considered what additional safeguards could be put in place to protect individuals.

Finally, legitimate interests can't always be used. It isn't a lawful justification for processing special or sensitive categories of data or for processing carried out by public authorities.

5.3 Necessity for fulfilment of contract

This can be used in two scenarios:

1. Where processing is necessary to complete a contract of which your client is a party. For example, when your client invests via a platform it will be necessary for you to provide information to the platform to complete your contractual obligations. The client will have terms in place with the platform which will include their own consents around marketing directly to them if they wish to do this. You do not need separate consent, however, to pass data to the platform.

2. Where there are certain steps you need to take before entering into a contract, where initiated by the prospective client. For example, a prospect sends you some basic financial information which you need to process in some way before deciding which level of service, if any, might be suitable for them as a client.

Clearly there are plenty of occasions, when acting on behalf of clients, where data would be processed under this legal basis.

5.4 Legal obligation

Where you are required by the FCA, the Financial Ombudsman Service or a court of law to provide information, you may do so under this exemption. Some law firms when handling claims will draft formal and intimidating letters insisting that you provide information, when they have no court order to compel this. You should think carefully, and seek advice, before providing data without a court order.

However, this clause is explicitly limited to legal obligations arising in the EU. This means requirements to disclose based on a non-EU court order may cause problems and legal advice should be sought on this point if the need arises.

5.5 Necessary for vital interests of the data subject

This is designed to cover life or death situations. It is unlikely to be relevant unless divulging health information on a client or employee in an emergency.

5.6 Necessity for performance of a task in the public interest

This is applicable to public authorities so not relevant for advisers.

5. The six lawful bases for processing data

Things to consider

- Keep a record of when client consent was obtained to process their data, particularly for marketing purposes. You will also need to document what will be done with their data and how long it will be kept for.
- Remember consent to data processing can't be built in as a condition of service. You should give clients a clear choice to both opt in and withdraw their consent.
- If you are relying on legitimate interest rather than consent, ensure data is being processed in the context of a relevant and appropriate relationship, and that it meets the reasonable expectations of clients.

6. Managing data

6.1 Privacy impact assessment

Carrying out a privacy impact assessment will focus your attention on what the most important and high-risk data processes you undertake are, and what actions you might need to take. Some of the key concepts you will need to consider when thinking about how you manage data under the GDPR are described below.

6.2 Minimisation, quality and accuracy

An important element of GDPR is what's known as 'privacy by design'. This means challenging whether your processes or your existing data retention policy takes into account your clients' privacy. It's worth asking whether all the data you currently hold is really necessary, and bearing in mind that what was relevant data to store two years ago may not be relevant now. Essentially you have to ask yourself: are you designing your processes with client privacy in mind?

The personal data you store and process should be limited to what is necessary for each specific purpose, and that data must be relevant as well as adequate.

The GDPR goes beyond the Data Protection Act in that it requires any inaccurate data to be deleted if it isn't updated, so if you have data that you don't need or use, then you should delete it. For example, if you have files from an old client bank bought without taking on the advice liability and they didn't become clients, then you are probably holding onto some higher risk data that you don't need to keep. Similarly, you may have fact-finds on customers who did not proceed to advice stage which can be deleted. Time for a spring clean on old clients' information.

If the information held is used for a purpose that relies on it remaining current, then the data should be kept up to date. This is almost second nature for advisers where an annual review is done for clients and fact-finds updated, but how often are changes made on paper notes but not updated on databases? For transactional clients, the ongoing accuracy of the information is less relevant, but if you still keep in touch with them there could be data you need to update, including their communication preferences.

There is a regulatory requirement to keep historic advice records which will contain data which is no longer current. Where this is retained and not used, it could be encrypted and archived to make it more secure and less likely to be inadvertently used by someone in your business.

To keep on top of your clients' communication preferences it is advisable to use a preference management tool. Many CRMs allow you to record and update preferences on their system, yet it's worth considering how best to allow clients to update their own preferences. There is already greater use of profile settings online on most systems, and these are a transparent and convenient way of putting your clients in control of the way you manage their data.

6.3 Records of processing activities

If you have more than 250 employees you will need to maintain internal records of all data processing activities your business undertakes. If you have 250 or less then you only need keep written records of processes relating to higher risk processing. Your client and personnel files will contain information on 'special category' data such as health and vulnerability. They will also contain the potentially high-risk information you might collate through Disclosure and Barring checks and Anti-Money Laundering Verification and financial crime checks, so you will need to maintain these records for client and employment information regardless of your size.

The record needs to include the following:

- Name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer).
- What the data processing is for.
- Description of the categories of individuals and categories of personal data.
- Categories of those who receive personal data.
- Details of transfers to other countries, including the safeguards in place.
- How long data will be kept.
- Description of your data security measures.

6. Managing data

6.4 Supply chain management

A lot of the work to prepare for the GDPR will involve managing your supply chain to ensure the third parties you pass client data on to for processing also understand their responsibilities under the new rules. You remain liable for the actions of those who process data on your behalf, referred to in the GDPR as 'sub-processors'.

Contracts

Unlike the Data Protection Act, the GDPR makes it mandatory to have a contract in place with any third party processor you pass data to. This includes technology suppliers, life companies, fund groups, DFMs and platforms as well as outsourced administrators, and potentially paraplanners, marketing and compliance people. This applies whether the processing is automated, for example a risk profiling or cashflow modelling tool, or non-automated, such as a DFM which is passed client information in order to construct a portfolio.

In addition to the responsibilities under the data processor contract checklist, a processor has the liability for:

- only acting on the written instructions of the controller;
- not using a sub-processor without the prior written authorisation of the controller;
- co-operating with supervisory authorities such as the ICO;
- ensuring the security of its processing;
- keep records of its processing activities;
- notifying any personal data breaches to the controller; and
- employing a data protection officer if required.

Failing to meet these obligations could result in damages in legal proceedings, fines or other penalties.

Crucially, if you pass your own processing obligations to a third party who gets it wrong, you remain directly liable to the client for fulfilment of these obligations. As when outsourcing compliance or paraplanning, you can build in terms into contracts with third parties which allow you to claim damages from them should you be sued or fined for their negligence, but those third parties cannot take direct responsibility and stand in your place even if they were at fault.

Buying or selling client data

This most commonly occurs when buying marketing lists or leads. You can only sell a marketing list if you have the consent of individuals to do so. This consent needs to be specific, and consent to a third party such as yourself contacting them, not just the business selling the list.

This additional consent should look something like this:

> We would also like to pass your details onto [name of company/companies who you will pass information to]/ [well defined category of companies], so that they can contact you by post with details of [specify products]/ [offers]/[services]/ [competitions] that they provide. If you consent to us passing on your details for that purpose please tick to confirm:
>
> I agree ☐

When buying a direct marketing list you will need to undertake due diligence on the seller, asking questions such as:

- Who compiled the list? When? Has it been amended or updated since then?
- When was consent obtained?
- Who obtained it and in what context?
- What method was used, for example, was it opt-in or opt-out?
- Was the information provided clear and intelligible? How was it provided, such as behind a link, in a footnote, in a pop-up box, in a clear statement next to the opt-in box?
- Did it specifically mention texts, emails or automated calls?
- Did it list organisations by name, by description, or was the consent for disclosure to any third party?
- Has the list been screened against the Telephone Preference Service or other relevant preference services? If so, when?
- Has the individual expressed any other preferences regarding marketing calls or mail?
- Has the seller received any complaints?
- Is the seller a member of a professional body or accredited in some way?

Any reliable vendor should be able to answer these questions easily as they are those suggested in the ICO's direct marketing guidance at https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf. If you buy leads on an individual basis, for example from VouchedFor or Unbiased, the same requirements apply.

6. Managing data

Example: Purchasing a client bank

It's easy to think advisers rarely buy or sell marketing lists or client data. However where a client bank, or goodwill, rather than the equity in a business is acquired, that's exactly what is happening. As you cannot bulk novate across adviser charges, you must get each client to agree to pay you an adviser charge under your own client agreement. This means you are effectively buying a marketing list from the seller and little more (other than any trail commission still being paid).

The best way to manage this is to encourage the selling adviser to help by contacting clients, advising them of the sale of the business, explaining who the buyers are, and explaining the process for signing new client agreements. Clients should be given the right to object to this and their information should not be passed across to the buyer if they do.

Before any data is passed across, the diligence questions above should be posed to the buyers to check that relevant consents are in place and under the GDPR this should become more commonplace.

Storing and passing data outside the EU

If you store or pass data to third party processors outside the EU you will need to satisfy yourself that they will protect your client or employee data with the same rigour as within the EU. Using a website or cloud service where the data is stored outside the EU means you are transferring data outside the EU.

Establishing this is not simple, and is likely to be an ongoing exercise. For example, the position on the adequacy of the US's 'equivalent' data protection framework has changed, as have the frameworks themselves.

The US previously operated the Safe Harbor framework, which was an agreement between the European Commission and the US, and gave some comfort that data was protected adequately by subscribers to Safe Harbor. US businesses voluntarily self-certified that they complied with the framework. In October 2015 the Court of Justice of the European Union issued its judgment in Schrems v Data Protection Commissioner (Ireland) which removed the assurance that using Safe Harbor had previously given to businesses, ruling it did not provide adequate protection.

Subsequently, the EU-US Privacy Shield replaced the Safe Harbor framework. It is a binding legal instrument under European law which can be used as a legal basis for transferring personal data to the US. In July 2016, the European Commission issued its formal adequacy decision on the Privacy Shield, confirming it was stronger than Safe Harbour and came into force from 1 August 2016. Bear in mind though that Privacy Shield compliance is voluntary and based entirely on self-assessment.

You can check which US firms are signed up to Privacy Shield at https://www.privacyshield.gov/list and look at what protection this offers at http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf. It includes global businesses providing cloud services such as Dropbox and Microsoft.

These are useful, mutually agreed substitutes for the GDPR, but not every country will have these in place and you will need to check through contractual terms in detail to ensure adequate protection is in place and you and your clients have legal recourse should this prove to be inadequate.

There are no model contract clauses for international data transfer under the GDPR yet, but the ICO provided guidance on these under the Data Protection Act at https://ico.org.uk/media/for-organisations/documents/1571/model_contract_clauses_international_transfers_of_personal_data.pdf and on how to assess international adequacy at https://ico.org.uk/media/for-organisations/documents/1529/assessing_adequacy_international_data_transfers.pdf.

! Things to consider

- Ensure that client data is kept up to date. If you have data you don't need or don't use, delete it.
- Where you're keeping hold of historic advice records, consider encrypting or archiving this data to make it more secure.
- Consider how to allow clients to manage the way you process their data and communicate with them.
- Keep a record of data processing activities your business carries out, in relation to both clients and staff.
- Remember you are still liable for data protection even where you pass data to a third party.
- Make sure where you're selling client data you have specific consent from clients to do this. If you're buying a marketing list, carry out appropriate due diligence on the seller.
- If data is being passed or stored outside the EU, understand how the third party is protecting client and employee data. Keep this under review.

7. New consumer rights

7.1 Rights of access, rectification and data portability

Where the legal basis for processing the data is based on consent or for the performance of a contract and where the processing is carried out by computer, your clients can request you transfer their personal data to them or to another data controller.

There is no need to take on new technology which is compatible with the receiving organisation, so this is not a way of forcing through seamless platform or back office migration. But data does need to be transferred in a structured, commonly used format which can be opened on a computer.

In addition:

- Data must be provided free of charge, unlike the existing £10 maximum fee for subject access requests under the Data Protection Act.
- You must provide the data within one month of receipt, extended to two months for complex or multiple requests.
- You will need to redact any information or data which would prejudice the rights of any other individual. This means removing or anonymising information about someone other than the person making the request.

Requests for correcting inaccurate data must be undertaken in the same timescales as a request for access and again with no charge.

You must react promptly to these requests and do so for free, so it's worth assessing how good your CRM is at exporting all client data where necessary, as well as deleting and archiving records.

7.2 Rights to erasure and to restrict processing

The right of erasure is an important new right, and one which some large businesses will struggle with as data will be held in several locations. As a regulated firm, it poses a problem given your regulatory obligation to hold client records for a minimum of five years under MiFID II and for many firms indefinitely in case of a future complaint.

The GDPR creates a number of exemptions whereby data does not need to be deleted. The most useful to advisers are:

- For compliance with a legal obligation, the performance of a task carried out in the public interest or in the exercise of official authority by the data controller
- For the establishment, exercise or defence of legal claims

The regulatory requirement to retain records supercedes the right to erasure where advice has been given, although there will inevitably be some data which can be deleted, such as those listed under 'Minimisation, quality and accuracy' above.

Given the potential for confusion over this issue, you may wish to make this point explicitly within your client agreement or privacy policy when covering client file retention or data processing. For example:

'As FCA regulated advisers we are required to retain records relevant to our advice to you and this can supercede your right to have all data deleted under the General Data Protection Regulation.'

The right to restrict processing allows someone to allow you to retain data but to restrict it from being processed. You should automatically restrict data from being processed where:

- someone contests the accuracy of the data you hold on them, while you verify it
- someone has objected to the processing and the legal basis used was legitimate interest, while you are considering whether your legitimate grounds override those of the individual
- if processing is unlawful and the individual opposes erasure and requests restriction instead
- if you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

Again, this is an area worth exploring with your CRM. It may be better for you to archive client data so that it cannot be used, but can be recovered and viewed in future, if necessary, possibly by a limited number of users.

7. New consumer rights

7.3 Right to be informed

Informing clients about how you process their personal data is usually best achieved through a privacy policy. Some advice on content and on how to present privacy policy information is contained within the Privacy Policy Design Guidelines, which features later in this paper.

7.4 Right to object

Under the GDPR there is a right to object to data being processed, but this will depend on which lawful basis you are applying. The right to object applies if you are processing data under the legitimate interest basis, but doesn't for data processing on a contractual basis.

Where applicable, your privacy policy must include details on how to object to processing and on request you must stop processing personal data unless:

- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

7.5 Rights related to automated decision making including profiling

There are further safeguards required where decisions are made automatically, without any human involvement. This may sound irrelevant, but you may have clients who are rejected for loans by an automated credit system, or screened out of a job in an automated recruitment process. If the decision could have a serious negative impact on an individual, or uses special category data then consent must be obtained and the right to challenge and object included, along with other safeguards. The growth of automated underwriting decisions means this could be a significant area for insurance business.

! Things to consider

- Clients can request access to their data – this must be provided for free within one month of the request. Correcting inaccurate data must be treated in the same way.
- Check with your CRM system provider about the ability to export client data and restricting data from being processed in certain circumstances.

8. Employment law issues

It's easy to forget that personal data doesn't just mean client data, it includes the records and data you hold about employed and self-employed staff as well. As with client data, you may be storing or transferring it outside the EU using a cloud-based system.

The data you hold on a personnel record is likely to include special category data, as you will probably hold information about your employees' health, possibly ethnicity, and maybe even biometrics.

Bear in mind non-special category information can be just as sensitive. Where employees leave under a cloud there may be requests to access personnel records, especially if negative references are provided. You will need to be vigilant and stick to the legal requirements when requests come through.

It is advisable to revisit employment and self-employed contracts to ensure they are up to date with relevant GDPR-compliant terms. You will also want to consider:

- Where staff information is stored. Data may be stored in multiple systems such as payroll systems, in addition to a file server. This should be audited in the same way as client data.
- Which members of staff have access to personal employee information, including third parties such as outsourced suppliers and professional advisers.
- What information can be deleted or archived, and what can be restricted.
- Your policy for monitoring email, and whether you have notified staff that this will happen.

Staff should be provided with a privacy policy, in much the same way as you provide one to clients.

Consent may not always be an appropriate legal basis and consent should not be simply added into a contract of employment as another condition to accept, in much the same way as it shouldn't be a compulsory condition of service in a client contract.

! Things to consider

- Revisit employment and self-employed contracts and make sure they are compliant with GDPR.
- Provide staff with a privacy policy as you would with clients.

9. Data processor contract terms

You must have a contract in place with anyone you pass data to for processing under GDPR. These are the terms you should include.

Compulsory terms

- the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);
- the processor must ensure people processing the data are subject to a duty of confidence;
- the processor must take appropriate measures to ensure the security of processing;
- the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
- the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- the processor must delete or return all personal data to the controller as requested at the end of the contract; and
- the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure they are both meeting their obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Compulsory details

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.

Good practice terms

- state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR; and
- reflect any indemnity that has been agreed.

10. Privacy policy design guidelines

We've all clicked and accepted privacy policies without giving them a second look. Make them a little easier to read and you'll avoid criticism and find them easier to update.

The ICO have old but still valid examples of good and bad practice here https://ico.org.uk/media/for-organisations/documents/1625136/good-and-bad-examples-of-privacy-notices.pdf. Here are some tips:

10.1 Think about the context

Most of us think of a boring piece of text on a link from a website footer, but you can provide a privacy policy orally, in print, on a sign or poster as well as by email or online.

It's generally best practice to deliver the privacy policy in the same medium you collect the personal information it relates to.

Using technology is a great way to make this more transparent, accessible and puts clients in control. A preference management tool is ideal for this, but blending a combination of techniques might work best.

10.2 Timing is important

You should be providing the policy at the most appropriate moment to allow a decision to be made. So collecting data via an online form and sending an email with the privacy policy afterwards isn't the right approach.

You might not be able to provide a privacy policy in an emergency. Telling people what you'll do with the information at a later point will suffice. Health information provided in a medical emergency is an example of this.

10.3 Layer the information

Use layers of headings, short sentences and fuller explanations to make lengthy text more accessible. This works best online.

For example

How will we use the information about you?

How will we use the information about you?

Process your order, manage your account, personalise your use of the website and post offers of other products and services we offer to you (if you agree).

May be shared with – members of our group of companies (if you agree). Won't be shared – for marketing purposes outside of our group. Please follow this link for further information.

How will we use the information about you?

How will we use the information about you?

We collect information about you to process your order, manage your account and, if you agree, post offers of other products and services that we offer.

We use your information collected from the website to personalise your repeat visits to the website.

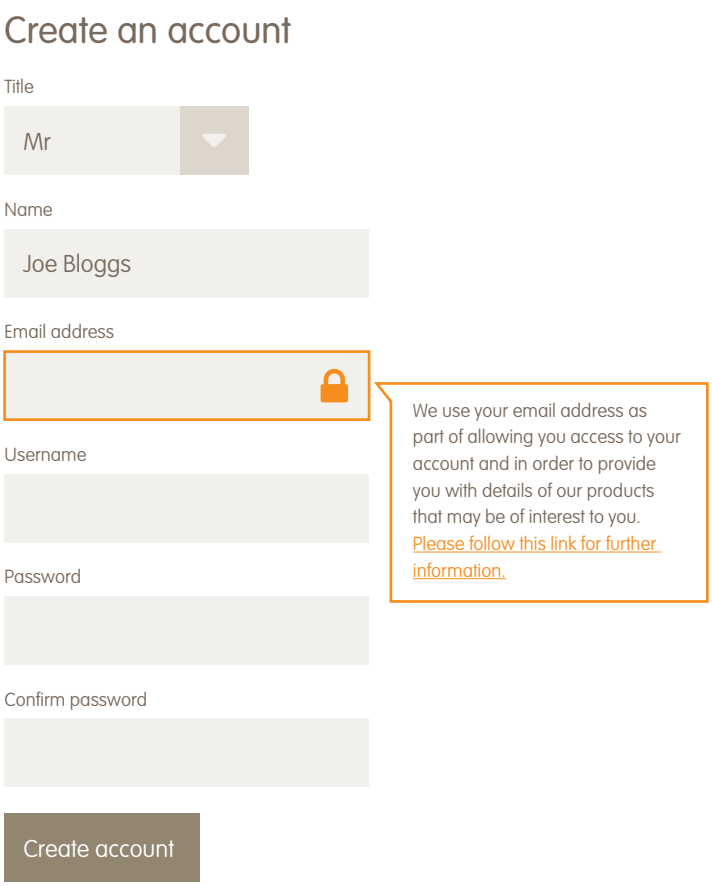
If you agree, we shall pass on your personal information to our group of companies so that they may offer you their products and services.

We will not share your information for marketing purposes with companies outside of our group.

10. Privacy policy design guidelines

10.4 Just-in-time notices

Again, these work best online as a method of delivering short, context specific messages relevant to the information someone is supplying. For example:



10.5 Consider mobile and video

Mobile usage is impossible to ignore. Alongside layering, which is very important for mobile, consider adding icons to assist navigation. Additionally, you could complement your written privacy policy with a more engaging video explaining your company policy.

The ICO provide guidance for app developers here https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf

10.6 View it from your client's perspective

When judging how much information should be upfront and how much can be put in a more detailed policy think about what you would expect as a client.

Consider issues such as:

- How sensitive is the information you are asking for?
- How likely would you be to object to how the information is stored or processed if you knew what would happen to it?
- Is there anything you wouldn't expect to happen to the data likely to happen to it?
- Is there any information you are not asking for which will have an effect on your service or advice?
- Are you going to pass the information to another organisation is a way that you wouldn't expect?

Questions like these will help you to decide which information should be brought into prominence with a client. Ideally, do some research and ask some clients what concerns them most and if there was anything they were surprised about after explaining what happens to their data.

10. Privacy policy design guidelines

10.7 Use of language

The ICO provides the following tips on the writing style used. Note the reference to your house style, values and principles. If your website is copywritten in a very informal manner, use of an abrasive, overly formal style can especially off-putting.

- Use clear, straightforward language;
- Adopt a simple style that your audience will find easy to understand;
- Don't assume that everybody has the same level of understanding as you;
- Avoid confusing terminology or 'legalese';
- Draw on research about features of effective privacy policies when developing your own;
- Align to your house style. Using expertise, for example in-house copywriters can help it fit with the style and approach your clients expect;
- Align with your organisation's values and principles. Doing so means people will be more inclined to read privacy policies, understand them and trust your handling of their information;
- Be truthful. Don't offer people choices that are counter-intuitive or misleading;
- Follow any specific sectoral rules as well as complying with data protection law, for example in advertising or financial services sectors; and
- Ensure your privacy policies are consistent across multiple platforms and enable rapid updates to them all when needed.

10.8 Consider vulnerability

We've already noted children are subject to additional controls, as they cannot give consent. There may be further safeguarding issues which mean more detailed or specific disclosures and explanations are required for certain individuals.

Some of the techniques suggested here might not be suitable for vulnerable people. You will need to think how you communicate differently with those people, taking into consideration the useful guidance issued by the FCA in recent years on this subject.

You may need to consider if privacy policies need to be issued to third parties such as attorneys acting with a Power of Attorney.

There may also be legal requirements in some countries to provide a version of the policy in another language. Even if it is not a requirement, if your client's first language is not English it is best practice to provide a translation.

10.9 Test it and keep it under review

We've already stated the benefits of viewing a privacy policy through your clients' eyes and gaining feedback. It is a document that will change as often as your data processes change. Given the rapid development of online marketing and the use of technology, you should consider whether you need to change your policy each time you adopt a new technology or service.

11. B2C direct marketing consents

Form of communication	Applicable regulations	Consent mandatory for unsolicited marketing?
Paper and post	GDPR Mail Preference Service	No, legitimate interest can be used with opt out
Email	GDPR ePrivacy Regulations	Yes, unless done in the context of the sale of a product or service.*
SMS	GDPR ePrivacy Regulations	Yes, unless done in the context of the sale of a product or service.
Social media	GDPR ePrivacy Regulations	Yes, unless done in the context of the sale of a product or service.*
Instant and social messaging	GDPR ePrivacy Regulations	Yes, unless done in the context of the sale of a product or service.*
Telephone	GDPR ePrivacy Regulations Telephone Preference Service Corporate Telephone Preference Service	Yes, unless done in the context of the sale of a product or service.* Consent must also be given to record calls.
Facsimile	GDPR ePrivacy Regulations Facsimile Preference Service	Yes, unless done in the context of the sale of a product or service. *
Cookies	GDPR ePrivacy Regulations	Yes, unless done in the context of the sale of a product or service. *

*There is no requirement for consent, only an opt-out, if the communication is done 'in the context of the sale of a product or service.' in the draft ePrivacy Regulations, this is a modification of the Privacy and Electronic Communications Regulations exemption which applied during "negotiations of a sale". So the exemption only applies where there is an activate attempt to purchase a product or service, not for pure, unsolicited marketing where it would not be reasonably expected.

There are other regulations which will apply, including those for the content of the marketing itself such as the Advertising Standards Authority standards, FCA rules on advertising regulations and financial promotions.

12. Conclusion

There is a lot to get to grips with on GDPR, but it's worth remembering the main aim of the new rules is to make sure people have control of their data. As an adviser, GDPR means understanding what data you have, and what you do with it.

GDPR has been described to me as an "important distraction", and that is true to some extent. But rather than focusing on the distraction element, perhaps there is a silver lining in all this. The review and due diligence processes required of GDPR provide a good opportunity to gain a better understanding and deeper insight into how your business works, and whether your processes are as efficient as they could be. One adviser has told me reviews carried out as part of GDPR compliance have actually led to their client agreement becoming more user-friendly as a result.

Many advisers will already be compliant with the Data Protection Act, and the GDPR is a natural extension of these rules for the digital age. What GDPR offers is a chance to consider everything in the round, from data security, to IT, to overall business continuity planning.

Whatever your thoughts about GDPR, this way of working is set to become the new normal. GDPR compliance is not a "one and done" exercise, but an ongoing piece of work to make sure your data processes are appropriate.

There is an increasing regulatory focus on ensuring good client outcomes, and the GDPR aligns with that. For financial planners, this concept will be nothing new.

We hope you find this white paper useful.

Natalie Holt
Content editor, Nucleus

Phil Young
Zero Support

13. Basic action plan

This is not a comprehensive list of everything a business must consider, as that will depend on the data and processing each undertakes, but should provide an outline of the main issues.

Accountability and governance	Notes	☑
Who is responsible for data protection and compliance with the GDPR within your business?		
Identify and document if and where you are a data controller and a data processor		
Do you have multiple people who need to be involved within different departments, for example, back office, accounts, marketing?		
What policies are already in place and do you need to amend or create them?		
Who will undertake a risk assessment of the business to prioritise which areas need attention and any deemed high risk?		
How is data protection trained into all staff both at induction and on an ongoing basis? Can you prove understanding and awareness within the context of your business, and not just generally?		
How will you audit compliance with the GDPR both now and in the future?		
Do you capture information about security breaches or process weaknesses which could be improved and how do you ensure they are acted on?		

Map your data and processes	Notes	☑
Do you have a central record or register which shows:		
Name of your business and data protection contact?		
Where all databases, spreadsheets or other data is stored?		
The sources of all personal data?		

13. Basic action plan

Map your data and processes	Notes	☑
All processes you undertake on personal data?		
Purposes of the processing?		
Description of the categories of individuals and categories of personal data?		
Categories of recipients of personal data?		
Details of transfers to other countries including documentation of the transfer mechanism safeguards in place?		
Retention schedules?		
Description of your security measures to protect the data?		

Establish the legal basis	Notes	☑
Have you established the legal basis for each data process?		
Do you have the necessary evidence to prove each legal basis (including children's data)?		

Conduct a Privacy Impact Assessment	Notes	☑
For each area where data is stored can you evidence:		
What personal data is held, and is it high risk/ 'special category'?		
If special category have you obtained consent and can you prove this?		
Who has access to the data?		
What is it processed for?		

13. Basic action plan

Conduct a Privacy Impact Assessment	Notes	☑
Can you erase data on request, and how?		
If erasure is not possible can data be encrypted?		
Can it be ported to another data controller, and how?		
Can you respond to a data subject access request in a timely manner, and how?		
Would you know if the security of the data or system was breached?		
Would you be able to notify a breach in time?		

Supply chain management	Notes	☑
Do you have a written contract in place with all other data processors?		
Does that contract include all required information as per the data processor contract checklist?		
Can they evidence how data will be deleted or made portable on request?		
How do you transfer data to third party processors and how secure is that process?		
Is any data transferred or stored outside the EU and if so what further safeguards have you established?		
Have you considered the employment law implications? Are new privacy policies or disclosures required?		

Secure your data – physical and digital	Notes	☑
Do you have an up to date information security policy covering items such as:		
IT management – resources, responsibilities and policy management?		

13. Basic action plan

Secure your data – physical and digital	Notes	☑
Access to data – how is it controlled?		
Network security?		
Secure data transfer – encryption, different types of media?		
Secure data storage – encryption, mobile device?		
Vulnerability management – physical security, penetration testing?		
Monitoring, testing and auditing control measures?		
Use of personal devices – personal mobiles, laptops etc on the server?		
Use of portable media – USB, CDs?		
Safe disposal of data – shredding?		
A clear, written disaster recovery plan? Is it tested?		
Are security events, incidents and breaches reported, recorded and acted on?		

Revisit consent and privacy disclosures	Notes	☑
Where required and for all marketing material have you:		
Decided where consent is required as the legal basis?		
Reviewed how you obtain consent and updated information in line with the GDPR?		
Ensured consent is not obtained as a condition of service?		

13. Basic action plan

Revisit consent and privacy disclosures	Notes	☑
Clearly separated out different consents for different processes?		
Created different opt ins for different forms of communication such as email, post, SMS?		
Do you record how and when all consents were given?		
How and where do you manage and record client communication preferences? How do clients update it?		
Have you made it as easy to withdraw consent as give it?		
Is your privacy policy up to date, and rewritten in plain English?		
Do you understand how all processes on your digital media work, such as cookies, to ensure your privacy policy covers all aspects?		

B2C direct marketing	Notes	☑
Where consent is required have you:		
Obtained it clearly and separately from the terms of the service?		
Obtained separate consent for each form of communication?		
Obtained separate consent for any data profiling?		
Recorded the time of date of each consent given?		
Made it as easy to withdraw consent as give it?		
Ensured any withdrawal of consent is recorded and will be excluded from future marketing?		

13. Basic action plan

B2C direct marketing	Notes	☑
If using lists or leads from third parties, have you:		
Checked the seller is a member of a professional body, or is accredited in some way?		
Obtained proof of opt-in consent within the last six months which specifically named or clearly described you, before using bought-in lists for texts, emails or recorded calls?		
Checked that the product, service or ideals marketed are the same or similar to those that the individuals originally consented to receive marketing for?		
Only used the information on the lists for marketing purposes?		
Deleted any irrelevant or excessive personal information?		
Screened the names on bought-in lists against your own list of people who say they don't want our calls (suppression list)?		
Carried out small sampling exercises to assess the reliability of the data on the lists?		
Established procedures for dealing with inaccuracies and complaints?		
When marketing by post, email or fax included your company name, address and telephone number in the content?		
Told people where you obtained their details?		
Provided people with a privacy policy (where it is practical to do so)?		
Tied the seller into a contract which confirms the reliability of the list and gives the ability to audit?		

13. Basic action plan

B2C direct marketing	Notes	☑
And, did the seller verify that the people on the list:		
Gave specific consent to receive marketing from you (or a clearly defined category of organisations fitting your description)?		
Were provided with readily accessible, clear and intelligible information about how their contact details would be used (such as privacy policies were easy to find and understand)?		
Were offered a clear and genuine choice whether or not to have their details used for marketing purposes?		
Took positive action to indicate their consent (for example they ticked a box, clicked a button or subscribed to a service)?		
Gave their consent reasonably recently (within the last six months)?		
In the case of texts, emails or automated calls, gave specific consent to receive marketing by those means?		

14. Further information

Preparing for the General Data Protection Regulation, Information Commissioner's Office

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Data protection checklists, Information Commissioner's Office

https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/

Guide to special category data, Information Commissioner's Office

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

The Data Protection Act (guide for consumers)

https://www.gov.uk/data-protection

GDPR full text as at 4 May 2016

http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Illuminate GDPR Technical Studio

https://illuminate.nucleusfinancial.com/technical-studio/gdpr/

15. Finding out more

Nucleus

Nucleus is an award-winning, adviser built wrap platform. Since launch we've established ourselves as a major force for change in the market. We're a thriving community of over 400 adviser businesses who currently manage over £13bn of client assets. For further details please go to www.nucleusfinancial.com.

We hope you've found this white paper of value.

For more Nucleus publications, please visit www.nucleusfinancial.com/support/publications.

Zero Support

Zero Support helps business owners and board members to tackle problems and develop ideas in their business. Prior to establishing Zero Support Phil Young was the MD of threesixty offering support to adviser firms for over 20 years.

For more information please go to www.zerosupport.co.uk.

Can we help?

For any more information on Nucleus please contact your regional business development director.

Darren Lowry
Account director
e: darren.lowry@nucleusfinancial.com
m: 07803 171 958

Mike Wallis
Account director
e: mike.wallis@nucleusfinancial.com
m: 07803 149 751

Chris Macdonald
Regional business development director: Scotland
e: chris.macdonald@nucleusfinancial.com
m: 07595 820 112

John Daly
Regional business development director: Northern Ireland
e: john.daly@nucleusfinancial.com
m: 07714 900 703

Russell Dowd
Regional business development director: North England
e: russell.dowd@nucleusfinancial.com
m: 07739 340 473

Amira Norris
Regional business development director: Midlands
e: amira.norris@nucleusfinancial.com
m: 07712 551 838

Alan Jordan
Regional business development director: South west
e: alan.jordan@nucleusfinancial.com
m: 07715 090 223

Martin Clement
Regional business development director: London and south
e: martin.clement@nucleusfinancial.com
m: 07739 339 908

Alex Pemble
Regional business development director: London
e: alex.pemble@nucleusfinancial.com
m: 07568 129 310

Notes

Notes

0131 226 9800 tellmemore@nucleusfinancial.com @nucleuswrap www.nucleusfinancial.com