White Paper

GDPR for IFAs:

6 Steps to Achieve Compliance

A guide for the implementation of GDPR processes and procedures at small to medium-sized IFA practices, commissioned by Gamble, Gaunt & Mole LLP Independent Financial Advisers

Gamble Gaunt & Mole
Independent Financial Advisers

WHY & WHEN DOES THE LAW CHANGE?

At the beginning of 2018, 74% of Europe's overall population of 843 million people was using the Internet [1]. The risk of cyber attacks and the unregulated use of personal information for marketing purposes have sadly become part of everyday life.

It was inevitable that something was needed to regulate the safety of the enormous amounts of personal information harvested by the world of business.

The European General Data Protection Regulation, "GDPR", will be enforced from the 25th May 2018 to overhaul the no-longer-fit-for-purpose Data Protection Act 1998 on how businesses process and handle the personal data of their clients and to strengthen the privacy rights of EU citizens.

The new regulations will be far more demanding than the previous provisions on data protection, and there will be steep penalties for non-compliance.

Brexit will not put a stop to the new law. One of the main goals of GDPR is to unify the EU data laws, however, the UK will not be exempt following its departure from the EU. A large part of the GDPR was drafted here in the UK, and the Government has already confirmed that its introduction will go ahead despite of Brexit.

Gamble Gaunt & Mole
Independent Financial Advisers

Size does not matter. Whether you are a business of just 1 or 1000 employees, if you are offering products or services and collect data from EU citizens, GDPR applies to your business.

AM I THE ONLY ONE WHO'S NOT READY?

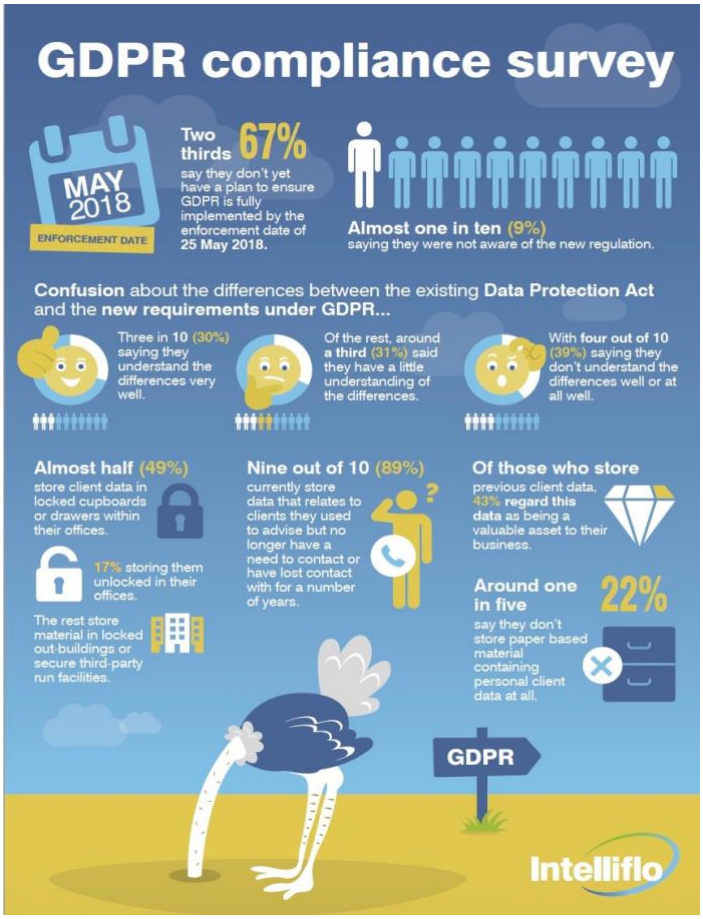
Have the impending changes been keeping you awake at night of late or at least been nibbling uneasily at your subconscious for quite a while now?

Or, is all of this complete news to you?

You are not alone.

A recently conducted survey [2] by the online adviser software provider Intelliflo has found that, despite the fast approaching enforcement date, 67% of their financial adviser clientele admitted that they did not have a plan in place to ensure that the new regulation is fully implemented by May.

One in ten even said that they had never heard of GDPR.

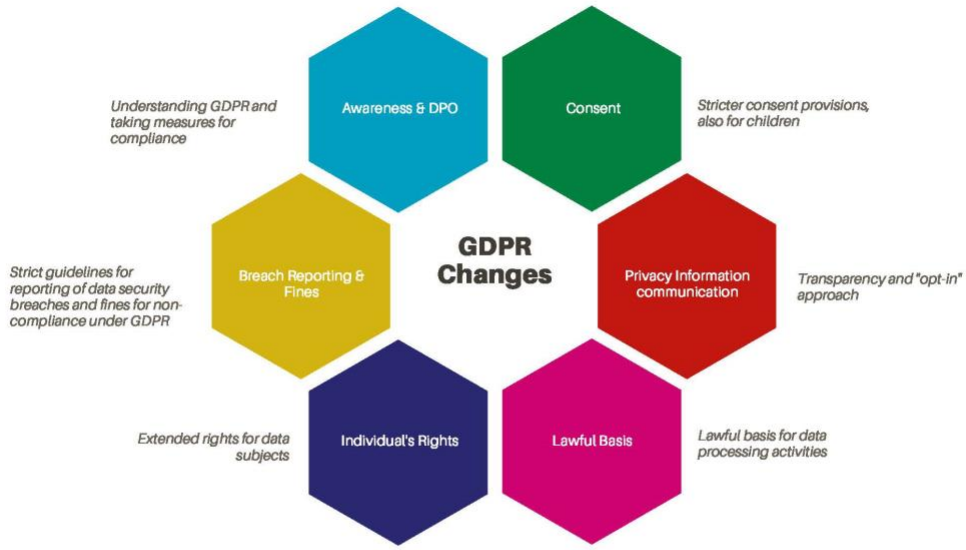


This head-in-the-sand reaction within the industry is most likely a direct result of the ongoing confusion about what will be different under GDPR, why the changes are needed and what the exact impact will be on the Financial Services Sector.

WHAT WILL CHANGE?

"GDPR widens the data rights of individuals considerably, and requires businesses to have transparent and clearly-worded policies and procedures in place to protect personal data, and take the appropriate technical and organisational steps to do so."

Gamble Gaunt & Mole
Independent Financial Advisers



"GDPR widens the data rights of individuals considerably, and requires businesses to have transparent and clearly-worded policies and procedures in place to protect personal data, and take the appropriate technical and organisational steps to do so."

Governance Obligations

As a data controller you have to be **fully aware** of the impact of the new law **and prove** that you have implemented all the necessary steps and reasonable action to ensure **compliance** with all aspects of privacy and data protection (Accountability Principle)

A Data Protection Officer has to be appointed where required and relevant procedures and documents have to be in place by May 25th 2018.

Consent

Under GDPR, the rules about **obtaining consent** are subject to **additional conditions**. Consent arrangements have to be kept separate from other written agreements and presented in an opt-in format. The agreement has to show that consent has been freely given whilst the client has been fully informed at the same time about what is involved in holding their data and that they have the right to withdraw at any time.

Gamble Gaunt & Mole
Independent Financial Advisers

The rules on how to handle consent for **children's data** have been tightened.

Privacy Notices

Privacy Communication has to be more clear and specific when explaining the processing of personal data than under the DPA 1998, to adhere to the transparency principle. You must provide the information in a concise, transparent, intelligible and easily accessible way using clear and plain language.

Lawful Basis

You have to review and confirm the **lawful basis for data** you hold, i.e. it has to be relevant for your processing activities and needs to be accurate at all times. The processing of special categories of data, such as racial or ethnic origin, political opinions, religious beliefs, trade union memberships, or health status and sexual orientation, is prohibited unless you can show a legal basis for processing. In most cases, explicit consent for holding such data should be sufficient.

Data Subject Rights

Individuals will have **more rights** to control the data you hold.

They gain the **right to be forgotten,** which means that they can request that the data you hold should be erased at their request. However, as this is not an absolute law, erasure can be refused on legal grounds. GDPR should not contradict existing law. If there is a legitimate reason to retain the data then this overrules the GDPR.

The individual has the **right to restrict processing** while a complaint about the legitimacy or accuracy of the processing activity is investigated.

The data subject has the **right to object** to the processing of their data for direct marketing purposes.

The introduction of the **right of data portability** allows data subjects to take greater control over the data you hold on them. They can request that their data should be moved from one provider to another or simply ask to view the data you have.

Such **subject access requests** have to be processed **within one month** of receipt and have to be free of charge.

The data has to be in **format** that can be **easily received and read** by the recipient.

Breach Reporting & Fines

Any **breach of data** has to be **reported within 72 hours** to the ICO. If the breach constitutes a risk to the rights and freedom of a person, i.e. exposes them to possible identity theft, fraud, financial losses, reputational damage or loss of confidentiality, the individual concerned has to be notified at the same time.

Non-compliance will be met with **massive fines**. You could be charged up to €20 million or 4% of your annual global turnover! So, better be on your toes.

WHAT DO I HAVE TO DO?

A lot of scaremongering has surrounded the change in law so far and caused confusion about what is actually to be done to be ready for May 2018.

There is no getting round the fact that a lot of work has to be done to ensure that you are compliant, however, the new regulations and their demands can be easily met if you follow a detailed plan of action.

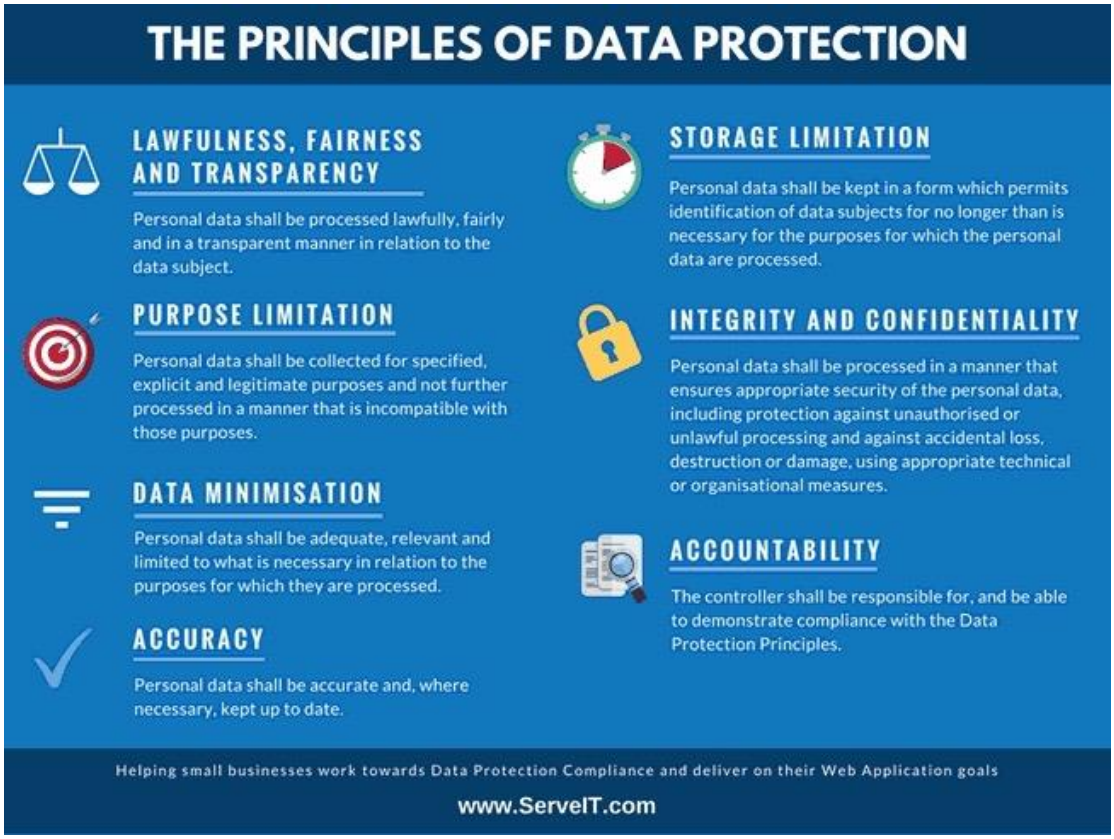
The ICO has developed a self-assessment tool on its website that you can use to check your compliance. However, as this is not specific to IFAs, we have compiled a shorter version that is applicable for your business.

1. Governance Obligations – Awareness, Measures & DPO

Whether you are a one-man business or a partnership, in order to implement and maintain the appropriate policies, you need to make everybody involved in your business aware of the GDPR regulation requirements.

Accountability

The GDPR Data Protection Principles are similar to DPA. However, you now have to be responsible for and be able to demonstrate compliance with all the principles.



Source: ServeIT

To ensure that you are compliant with all GDPR principles, it is important that you review your DP policies and code of conduct:

- Carry out an audit of all existing personal data to determine what kind of data you hold, where you hold it, in what format, where you obtained it from and what the lawful basis is for processing each data category.

- Create and maintain a visible process to show that you are complying with the accountability principle. This should include codes of conduct, audit trails of data processing decisions, staff training materials, and privacy impact assessments (PIAs).

Data Protection Officer

Under the new regulation you have to appoint a Data Protection Officer (DPO) “in some circumstances”. The final draft has left the definition of these “circumstances” rather vague and open to debate.

However, regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has the staff and skills to be compliant

under the GDPR. As a data controller who handles sensitive data such as health, financial and employment information, you should therefore appoint a partner or an external adviser to take responsibility for the implementation and maintenance of compliant governance.

Most likely, you will already have an appointed Compliance Officer or Consultant in your organization. It would make sense to add data protection maintenance to their role.

Should you decide to appoint a DPO in-house, it is advisable for them to attend a training course, of which there are many. Check out the web to see what is available both online and locally.

The DPO has to be familiar with all the requirements of data protection and safety in your organisation and has to act accordingly.

Article 39 defines the minimum tasks as:

- “To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.”

- “To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.”

- “To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).”

It is very important to be aware, however, that it is not the DPO who is personally liable for any infringements, but the data controller, i.e. the IFA practice. Therefore chose your responsible person or consultant wisely.

Once you have appointed a DPO and he or she has ensured that everybody in your organization is aware of GDPR and its impact on your business, you are set to implement the measures required to fulfil your governance obligations.

International

The transfer personal data outside the EEA remains restricted. If you are dealing with such transactions, determine your lead data protection supervisory authority. For this, you can refer to Article 29.

2. Update your Consent Format

Review your consent communication process to ensure that you are compliant with the new rules.

- Adopt an opt-in approach, i.e. do not rely on pre-ticked boxes or inactivity.

- Make it a separate entity to other written agreements and ensure that you use clear and plain language.

- Advise clients of their right to withdraw consent at any time and that this is a simple process.

- Ensure that the data is required for the processing of a contract. Otherwise the consent becomes invalid.

- Ensure that you have separate consent agreements for each processing operation.

- Review your policies relating to children and verify their ages to obtain either the parental/guardian consent or the child's consent for any data processing activities.

3. Update Your Privacy Information Communication

Most IFAs currently use a general clause such as "Do you give us permission to hold and process personal data on your behalf?"

This will no longer suffice once GDPR comes into force. You need to change your communication so that it clarifies what data you hold, how long you hold it for and what the purposes are you are going to use the data for.

You also have to make individuals aware of their right to complain to the Information Commissioner's Office (ICO) if they believe that there is a problem with the way you are handling their data. This information needs to be concise, easy to understand and written in clear language.

Review your privacy notices to ensure that they meet the fair and transparent processing requirement. Use clear and plain language and make them easily accessible.

If you have a contact form on your website, add a notice to explain why you are collecting the data and for what purpose. State clearly whether the data is passed on to third parties or not.

Should you use third parties to collect data for you, ensure that the responsibility for review, update and approval of the privacy notice is assigned to them.

4. Lawful Basis for processing personal data

As under the previous regime, you must have a valid lawful basis in order to process personal data.

The 6 bases for lawful processing generally remain as they are, but there are some differences. You need to look at your existing processing, select the most appropriate lawful basis, and check that it applies. In many cases it is likely to be the same as your existing provision, most likely consent and contract.

If you haven't already done so, you now have to clearly document your chosen legal basis or bases (more than one is allowed) before the 25th May 2018.

It is important that you complete this exercise, as you will no longer be allowed to change your legal basis for processing after the introduction of GDPR and may find yourself to be non-compliant if this does not match your processing.

Also, under the GDPR more emphasis is placed on being accountable for and transparent about your lawful basis for processing.

This means that you must inform data subjects upfront about your lawful basis for processing their personal data. This has to be communicated to individuals by 25 May 2018 and included in all future privacy notices.

5. Ensure your data formats cover all the new Individual's Rights

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification

4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object

1. The Right to be informed

The right to be informed covers your obligation to provide 'fair processing information'. You should convey this through your privacy notice.

2. The Right of Acess (subject access requests)

Data subjects have the right to access their personal data and supplementary information to allow them to be aware of and verify the lawfulness of the processing.

3. The Right to Rectification

Individuals have the right to have personal data rectified if it is inaccurate or incomplete.

4. The Right to erasure (right to be forgotten)

Individuals have the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

Please note that a request for erasure of data can be refused on the grounds of compliance with a legal obligation.

5. The Right to restrict processing

Individuals have a right to restrict processing of personal data as follows:

- Where an individual contests the accuracy of the personal data. Restrict the processing until you have verified the accuracy of the personal data.

- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests). Consider whether your organisation's legitimate grounds override those of the individual.

- When 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.

In these circumstances, you are permitted to store the personal data, but not to further process it.

6. The Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services by moving, copying or transferring personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

You must be able to provide the personal data in a "structured, commonly used and machine-readable form". Open formats include CSV files (Comma Separated Values files).
You may be required to transmit the data directly to another organisation on request if this is technically feasible.
If the request concerns the personal data of more than one individual, you must take into account whether providing the information would prejudice the rights of any other individual.

7. The Right to object

Data subjects have the right to object to certain processing activities on "grounds relating to his or her particular situation".

The GDPR stipulates: "You must stop processing the 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."

Individuals have to be informed of their right to object "at the point of first communication" and in your privacy notice.

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

Concerning any of the above rights, it is advisable to have a system in place that enables you to have individual data ready on request, so that you are in a position to act without delay, as all requests have to be responded to "without undue delay", and within one month.

You cannot charge for the requested information

If you have disclosed the personal data in question to third parties, you must contact them and forward the details of the request (unless this proves impossible or involves disproportionate effort).
If asked to, you must also inform the data subject about these recipients.

6. Know What To Do In Case Of A Data Breach

It is important to ensure that you have the right procedures in place to detect, report, and investigate a personal data breach.

Breaches only have to be notified to the ICO, if they are likely to result in a risk to the rights and freedoms of individuals. This could be discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

In most cases where a breach is likely to result in a high risk to the rights and freedoms of individuals, the data subject has to be informed directly as well.

Failure to report a breach when you should do so could result in a fine, on top of a fine for the breach itself.

However, fines are always proportionate to the offence, and will take account of both the extent of negligence and the extent the organisation has gone to to deal with breaches and issues.
So, the better you are prepared the less the fine will be.

In conclusion, the GDPR is coming, and with less than 3 months to go, now is the time to tackle its demands.

The “head-in-the-sand” approach is no longer an option, given the hefty fines you could face if you are not meeting the mighty GDPR eyeball to eyeball.

Here is a brief summary of the action you should take:

- Check how your company is storing personal data and ensure that the methods being used are compliant.
- Review and adapt your privacy notices and consent agreements.
- Adapt your systems to support all data subject rights – be ready for any eventuality.
- Make sure everyone who handles personal data within your organisation understands the impact on your business.
- Choose third parties with whom you share your clients’ personal data very carefully; they have to be compliant too.

When in doubt, seek professional help. Don’t risk the penalties and potentially your business.

Gamble Gaunt & Mole
Independent Financial Advisers

References:

[1] https://wearesocial.com/uk/special-reports/digital-in-2017-global-overview

[2] https://cdn2.hubspot.net/hubfs/344772/images/Infographics/GDPR%20compliance%20survey_infographic.pdf?t=1518023100671

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

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_annex_en_40856.pdf (DPO FAQ)

About the author:

Caren Launus-Gamble is co-founder & director of the award-winning autistic web accessibility agency KreativeInc Agency in Leeds, West Yorkshire – Web Accessibility Design, Development, Training & Consultancy.

More information at: https://kreativeincagency.co.uk/