ICAS

PREPARING FOR GDPR
MARCH 2018

In association with BRODIES LLP

IMPORTANT NOTICE

This document is published by ICAS for information purposes only and should not be regarded as providing any specific advice. Recipients should make their own independent evaluation of this information and no action should be taken, solely relying on it. This material is not intended for distribution in any jurisdiction in which this would be prohibited. Whilst this information is believed to be reliable, neither ICAS or Brodies give any representation or warranty (express or implied) of any kind, as regards the accuracy or completeness of this information, nor do they accept any responsibility or liability for any loss or damage arising in any way from any use made of or reliance placed on, this information.

INTRODUCTION

The General Data Protection Regulation (or "GDPR") represents the biggest shake-up of data protection law in almost 25 years. GDPR comes into force on 25 May 2018, ushering in a new regime for how personal data must be handled, with a greater emphasis on transparency, and backed up with much tougher sanctions for breaches (with possible administrative fines of 4% of annual worldwide turnover).

CAs should already be taking data protection compliance seriously. ICAS Members enjoy a reputation of trust with clients and others, based in part on confidence that all personal data will be handled responsibly. Any failure to deal with personal data appropriately could lead to an erosion of trust, reputational damage, and a subsequent loss of business.

As more and more clients become aware of the value of their data and the risks that are out there, they will increasingly ask their CA to demonstrate that their information is being processed appropriately. In addition to client demand, expect insurers to be taking an equally keen interest in how data is being handled.

While some CAs will understandably be frustrated by the need to meet further statutory requirements, there are benefits for firms that are GDPR compliant. These include:

- increased client satisfaction;
- many work processes become more streamlined when unnecessary requests for information are removed;
- information becomes more easily accessible when only relevant data is retained; and
- competitive advantage over firms which aren't compliant.

In short, GDPR presents an excellent opportunity for a CA practice to be more efficient.

PURPOSE OF THIS GUIDE

ICAS has joined with law firm, Brodies LLP, to produce this Guide, which is intended to give introductory practical guidance and support to CAs on some of the main issues that we expect them to face when preparing for GDPR compliance. Given the scope of GDPR, and the varying way it will impact different firms, this is not intended as a complete guide to GDPR. To help you find more detailed answers, we have included links to external guidance and material, which will provide fuller information on key areas.

The template documents associated with this Guide are provided for firms to consider using as a starting point for development of their own documents. Firms are free to use their own documents or to take these templates in whole or part and develop or incorporate them into other documents.

If you have any questions about the Guide, please contact ICAS' Practice Support Team on 0131 347 0249 or email practicesupport@icas.com.

HOW WILL GDPR APPLY IN THE UK?

The General Data Protection Regulation (GDPR) has direct effect in all EU member states and does not need the UK Parliament to take action for it to apply in this country. However, as GDPR allows EU states limited scope to vary the way it is implemented, the Government has published a new Data Protection Bill that should become an Act of Parliament before GDPR comes into force in May this year.

For the purposes of compliance, data protection law in the UK will consist of GDPR as supplemented by the provisions of this Act. For simplicity, this Guide uses the term GDPR simply to refer to GDPR and the Act read together.

It is unlikely that Brexit will have any impact on GDPR – at least not in the next few years.

WHERE CAN I GO FOR GUIDANCE?

Guidance on the new law is published regularly by the UK's data protection regulator, the Information Commissioner's Office (ICO). CAs are encouraged to view the material on the ICO's website (ico.org.uk), as it contains helpful guidance for companies, produced with the aim of making GDPR compliance as straightforward as possible. For example, on 13 March, the ICO published guidance aimed at micro-businesses employing less than 10 people, which is likely to be very helpful to many CA firms.

Guidance is also available through the Article 29 Working Party (WP29), which is the regulators in all EU member states acting together. Once GDPR comes into force in May, the WP29 will become known as the European Data Protection Board, and will be the EU's authority on data protection.

If there are areas of GDPR that you think are particularly significant for your firm, you may wish to obtain advice from a solicitor, or someone else with sufficient knowledge of the incoming legislation.

FURTHER READING

ICO – Preparing for the GDPR: 12 steps to take now
ICO – 'Guide to the GDPR'
ICO – Guidance for Micro Businesses
WP29 website

WHAT IS MY BEST STARTING POINT FOR GDPR?

This Guide has been produced in the expectation that CAs will have reasonable knowledge of the current data protection legislation, and are broadly compliant with its requirements. Thankfully, GDPR represents evolution, not revolution, so responsible firms will not be starting from scratch in this exercise.

An important first step is to make sure you have a good understanding of all the different ways in which personal data is handled by your firm. You should bear in mind that partners and directors will not always be aware of what happens on a daily basis at the 'coal face' – it is a good idea to involve as many employees as possible in the exercise.

Once you know what you are dealing with, you can consider how each of the issues set out in the Guide applies to your firm, and what steps you need to take to bring you closer to GDPR compliance.

ACTION

Review the sample Excel Data Processing Register which is associated with this Guide. This is one example of how you could undertake a review of your firm's use of personal data

WHAT ARE THE MAIN PRINCIPLES FOR DATA PROCESSING?

CAs must ensure that all processing of personal data complies with the following data management principles, which require that data is:

- Processed lawfully, fairly and in a transparent manner
- Collected for clear and legitimate purposes and not further processed for incompatible purposes
- Adequate, relevant and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Kept only for as long as necessary for the purposes for which the personal data are processed
- Processed securely

These six principles should be the foundation for your preparation for GDPR. CAs are expected not only to comply with these principles – they must be able to demonstrate their firm's compliance (see Governance and Records later in this Guide).

If you handle personal data in a way which does not comply with one or more of the above principles, you run the risk of a complaint being made to the ICO.

IS MY FIRM A DATA CONTROLLER?

CA practices will generally exercise sufficient professional judgement and decision making over the purposes for which data are processed to be controllers of the personal data they process in the normal course of their business, even though they work on the general instruction of clients.
As controllers, firms will need to ensure that they:

- have a lawful basis for their processing activities in terms of GDPR;
- have provided the individuals whose data they process with the information which meets GDPR's transparency requirements by explaining how and why they are processing an individual's personal data (i.e. through an appropriate privacy statement, published on the firm's website, included or referenced within a letter of engagement, and otherwise referenced on forms or other channels for data capture); and
- only process personal data in accordance with the terms of these privacy statements.

However, CAs need to be aware that some services provided by firms – for example, those that involve payroll processing – may see the firm acting as a processor, with the client being the controller. Whereas the outgoing legislation does not impose direct statutory responsibility on processors, this will change under GDPR, with processors taking on many of the same responsibilities as a controller. For example, data processors now owe direct statutory responsibility for personal data security.

CASE STUDIES

EXAMPLE 1

Company A engages a CA Practice to provide book-keeping and accountancy services. The books and records contain personal data such as customer details. CA Practice will generally be the controller as the firm has professional obligations under the Code of Ethics (the fundamental principle of professional behaviour) which oblige them to take responsibility for personal data they process.

EXAMPLE 2

Company B engages CA Practice to provide a payroll bureau service. As CA Practice have no control over whose personal data is processed and simply execute the processing to provide the bureau service, then CA Practice will generally be a processor.

EXAMPLE 3

Company C uses cloud accounting services. Company C makes all the book-keeping entries but CA Practice assists in the preparation of quarterly VAT returns and to prepare annual accounts and tax computations. The cloud accounting software is hosted by the cloud accounting software provider but on a monthly subscription to CA Practice. CA Practice will generally be a processor in respect of the cloud services as Company C determines the purposes for which and manner in which personal data is processed. The cloud service provider would be a sub-processor. CA Practice may also be a controller, however, for its professional services as it can determine the manner in which personal data is processed when preparing VAT returns and accounts for Company C.

The situation may be more complex for insolvency practitioners where the IP may process personal data in a number of capacities.

WHAT IF A THIRD PARTY IS PROCESSING DATA ON BEHALF OF MY FIRM?

If you engage a third party to process client data on behalf of your firm, you will need to ensure that your contract with this party satisfies the requirements of GDPR. As you are still ultimately responsible for the proper processing of the data, you need to make sure the third party has a responsible attitude towards data protection.

CASE STUDIES

CLOUD SOFTWARE

A CA firm uses cloud software to prepare client accounts and tax returns. Personal data is uploaded by the firm to an online portal. Under GDPR, the cloud software provider is a processor, whilst the firm is the controller. In preparation for GDPR, the CA firm should ensure that its contract with the supplier contains the provisions required by GDPR for controller-processor contracts under Article 28. It should also be satisfied through its own due diligence that the service provider is reliable and competent to process the personal data in accordance with all of the requirements of GDPR. One particular issue will be ascertaining where the data will be hosted as many cloud providers host data outside the EEA, leading to further requirements under GDPR. Ultimately, any assessment should take account of the risks to the individual data subjects if issues arise.

ACTION

All live contracts which involve the processing of personal data to which a CA firm is a party, should be reviewed to ensure that the contract will comply with GDPR on 25 May 2018. If the contract will not satisfy the new law, you should negotiate with the other party to amend the contract accordingly

Review the style data protection clause which is associated with this Guide. This is an example of wording which you might expect to see in commercial contracts.

HOW CAN I BE TRANSPARENT ABOUT MY FIRM'S DATA PROCESSING?

Clients and other individuals who provide data to firms must be made aware of the ways in which the firm will handle their data. The easiest way to do this is to produce a 'privacy statement' which summarises the firm's approach to personal data.

Best practice would be to draw your clients' attention to the privacy statement through your letter of engagement. You can either include a copy of the notice, or advise where it may be found. Most privacy statements should be published on the firm's website. Consider also how privacy notices can be drawn to the attention of other individuals whose data you may collect and use.

While privacy statements are not new, GDPR requires more information to be included.

In addition to explaining your firm's activities to clients, you should consider drafting an 'internal privacy statement', to allow the firm's employees to understand how their information will be handled.

ACTION

If your firm already has a privacy statement, this should be reviewed to see if any changes need to be made.

If your firm does not have a privacy statement, one should be prepared.

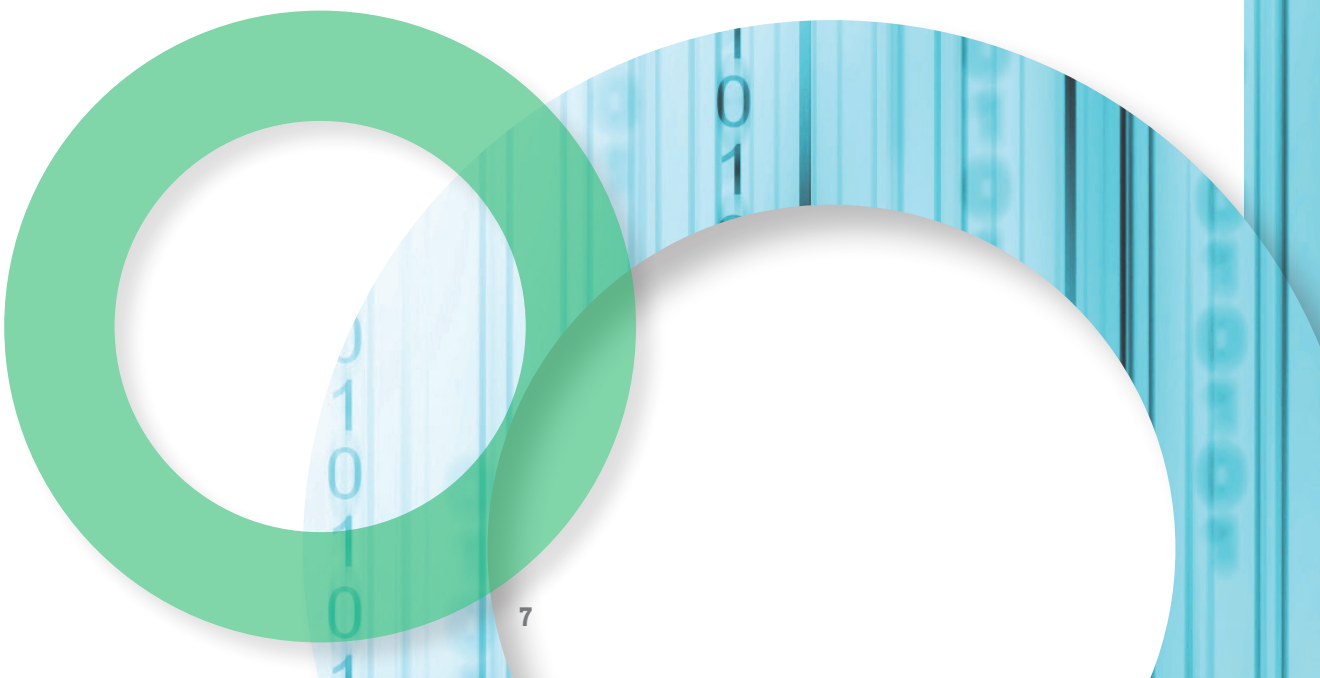
The same steps should be taken for 'internal privacy statements' for employees.

You may want to refer to the template privacy notices which are associated with this Guide.

It is also a good idea to review the privacy notices of other organisations; including ICAS.

FURTHER READING

ICAS privacy notice https://www.icas.com/privacy
'Guidelines on transparency' – "(see WP29 website)



DO I NEED SOMEONE'S CONSENT TO PROCESS THEIR DATA?

If you do any background reading on GDPR, you will soon find out that consent is one of the key focuses of the new law. However, consent is just one of the grounds on which personal data processing can be justified. CA practices will often rely on other grounds on which to process personal data. These may include the performance of a contract with the individual concerned – or because it is necessary to further legitimate interests of the practice or its clients (provided those interests are not overridden by legitimate privacy interests of the individuals whose data is being processed).

Where consent is most likely to be important is in the marketing activities of a CA practice.

In general terms, electronic direct marketing can be justified in three circumstances – (1) prior notified consent from the individuals concerned, (2) the so-called 'soft opt-in' (marketing to existing clients, but with the right to opt-out), and (3) to corporate subscribers.

Firms which are issuing marketing material to clients by email need to abide by these rules and, if relying on consent, be aware that, as the requirements for consent are stricter under GDPR, existing consents might not meet GDPR standards and may need to be refreshed.

Three of the most important points to note about consent under GDPR are as follows:

- consent requires an affirmative action by the individual – pre-ticked boxes will no longer work;
- consent must be freely given, and should not be an unnecessary pre-condition for the provision of other services; and
- consent wording must be sufficiently specific, so avoid general phrases such as 'for marketing purposes'.

CASE STUDY

EXAMPLE 1

A Manager is at a networking event and is provided with business cards by prospective clients and introducers. The contact details collected should not be added to the firms CRM database in the first instance. The manager may wish to email them to follow up the networking event and invite them to subscribe to communications that they may find useful in the future. A link can be provided to a communications subscription page.

ACTION

Review letters of engagement and, if necessary, update to ensure GDPR compliance – consider the style clause for letters of engagement which is associated with this Guide.

Identify categories of marketing activities (e.g. events, publications, tax cards)

Review existing arrangements for marketing activity

Put in place arrangements to obtain specific consents where necessary.

FURTHER READING

ICO – GDPR consent guidance

Guidelines on consent' – "(see WP29 website)

WHAT IS DATA MINIMISATION?

While data protection law has always required organisations only to collect personal data that is required for the purpose for which it has been collected, GDPR makes this even more important. Firms will need to ensure that they only collect and record personal data which is necessary for the purpose for which it is sought.

ACTION

Review all the personal data which the firm requests from third parties.

Ensure that the information requested is needed by the firm to complete its engagement.

Update forms to remove unnecessary data collection where appropriate.

HOW LONG SHOULD I RETAIN A CLIENT'S DATA?

One of the most important aspects of GDPR is ensuring that personal data is kept for no longer than is necessary for the purposes of the engagement. CAs are encouraged to ensure that their firms have appropriate data retention and destruction policies in place. These policies should be formalised, communicated to all employees, and implemented on an ongoing basis.

While data protection law does not mandate retention periods for personal data which will be processed by CAs, there will be some instances where documents must be retained for a certain period, to comply with other legislation (e.g. HMRC requirements).

ACTION

Review data retention and destruction policies.

Communicate data retention and destruction policies to employees.

Ensure that data retention and destruction policies are appropriately implemented by the secure destruction or proper erasure of data in accordance with those policies.

FURTHER READING

Guidance on retention periods is available in section 1.4.11 of the ICAS General Practice Procedures Manual

DOES MY FIRM NEED TO APPOINT A DATA PROTECTION OFFICER?

Firms should consider whether GDPR will require them to appoint a data protection officer. Many CA practices will not need to because the requirement is focused on public authorities and those who carry on, (i) regular and systematic processing of data on a large scale, and (ii) large scale processing of special category (formerly sensitive) data, or data relating to criminal convictions.

Please note, however, that even if there is no requirement to appoint a statutory data protection officer under GDPR, firms should allocate responsibility for data compliance to an appropriate individual who has the authority to carry through the necessary changes and to ensure compliance on an ongoing basis.

ACTION

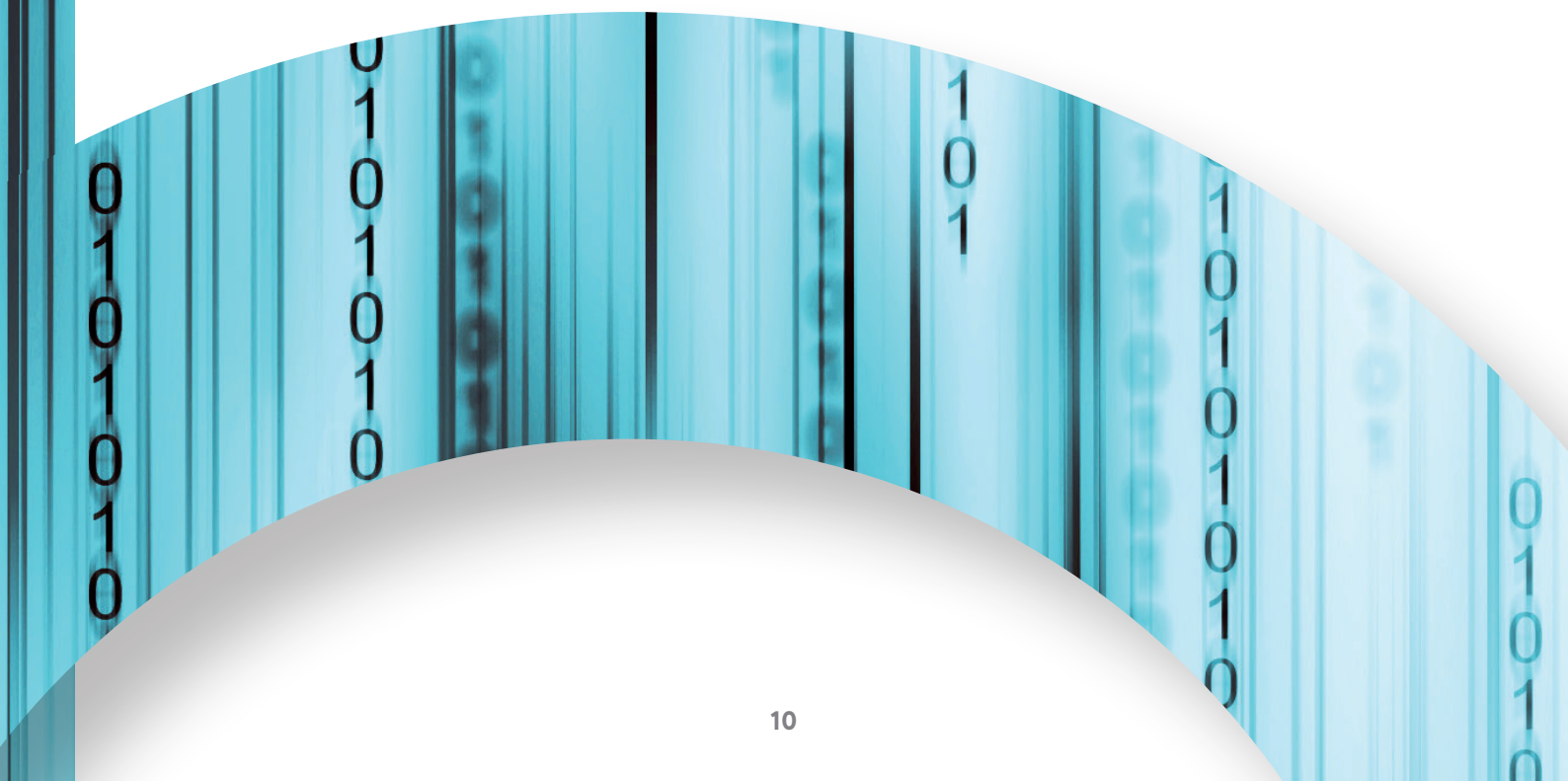
Consider whether there is a need under legislation for the business to appoint a Data Protection Officer.

Appoint a senior person within the firm to have responsibility for data compliance.

Ensure appropriate time and resource is given to data protection compliance (as with all compliance issues).

FURTHER READING

Guidelines on Data Protection Officers' – "(see WP29 website)



HOW CAN MY FIRM DEMONSTRATE COMPLIANCE WITH GDPR?

CA firms are not only expected to comply with the GDPR – they are expected to be able to demonstrate that they comply. A number of new responsibilities are included to reinforce that accountability. Consideration should be given to the following:

RECORDS

Firms must keep appropriate records of their data processing activities, which records may include:

- Data Processing Register*
- Register of Data Processors*
- Consent forms and evidence of consent
- Privacy statements
- Details of non-EEA data transfers
- Training
- Copies of relevant contracts
- Data Privacy Impact Assessments
- Policies and procedures
- Data breach register and procedures
- Information relative to the handling of data subject requests

A key component of the record-keeping exercise will be the maintenance of a data processing register, which lists all of the firm's processing activities, with appropriate GDPR analysis. Compiling this register may be one of the first steps you take towards GDPR compliance. A sample Excel Data Processing Register is associated with this Guide

Under GDPR, there is a limited exemption for small and medium-sized organisations. If your firm has less than 250 employees, you will only need to document processing activities in the registers asterisked above that:

– are not occasional; or

– could result in a risk to the rights and freedoms of individuals; or

– involve the processing of special categories of data or criminal conviction and offence data.

Further guidance from the ICO and WP29 as to the scope of that exemption is expected in due course.

POLICIES

Firms should adopt appropriate policies and procedures as part of appropriate and effective compliance measures. This should be more than simply having a data protection policy – important though that is. As personal data processing will occur in almost every area of a firm's business, firms should consider whether they have appropriate policies and procedures in place to regulate all aspects of the firm's operations that may be relevant to data protection compliance.

Policies and procedures which might be appropriate to have include:

- Information Classification
- Physical Security
- Intellectual Property
- Social Media
- Product Development
- Corporate Communications
- Third Party Contractors
- Contract Governance
- Data Retention and Destruction Data Quality
- Disaster Recovery/BCP
- Homeworking
- Personal data security/breach notification
- Acceptable use
- Data Privacy Impact Assessments

TRAINING AND AWARENESS

Firms should ensure that their employees understand the importance of personal data and their obligations to treat it responsibly and securely. Employees need to understand how the requirements of GDPR are relevant to the day to day work that they do. This will include making sure that they understand the requirements for data security and what to do if they identify an actual or suspected personal data breach, to make sure they can recognise data breaches, and respond accordingly (see Who do I need to notify if there's a data breach? on page 16). They also need to be able to identify requests by individual data subjects to exercise their rights under GDPR so that they can ensure that these requests are drawn to the attention of the correct person internally to be handled promptly and properly.

Effective compliance is more than just a tick box exercise, working best when it becomes part of an organisation's DNA. Cultural change is a key requirement if data protection is to be built into how organisations do things, and is not just a bolt on. That cultural change comes from the partners or directors. The ICAS Practice Support team can provide appropriate training.

DATA PRIVACY IMPACT ASSESSMENTS

Any firm which is proposing a new personal data processing activity must ensure that proper consideration is given to the potential risks to the individual data subjects. Where those risks are assessed as being high, the firm should conduct a DPIA. A DPIA is a documented process designed to ensure data protection compliance by assessing the validity, proportionality and necessity of what is proposed whilst managing and mitigating the risks to the individual. If following the DPIA process, the residual risks are still assessed as being high, processing must not start without consultation first with the ICO.

Even if a DPIA is not required by law, firms may find this to be a useful way to ensure that new activities do not lead to unintended risks to personal data.

FURTHER READING

WP29 – Guidelines on DPIA and determining whether processing "is likely to result in a high risk" for the purposes of GDPR (see WP29 website)

DO I NEED TO CHANGE MY FIRM'S DATA SECURITY MEASURES?

The basic security standards expected to be met for personal data are broadly equivalent to those required under current data protection law. If there is a data breach, the firm will be expected to be able to demonstrate that it had appropriate measures in place to ensure a level of security which was appropriate to the risk. GDPR specifically refers to particular measures by way of examples:

- pseudonymisation is a masking technique which involves replacing identifying characteristics of data with a pseudonym or artificial identifier (e.g. using client numbers, instead of names), so that the individual cannot be directly identified;
- encryption – many organisations now require all attachments containing personal data to be sent in encrypted format;
- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore personal data in a timely manner in the event of a physical or technical incident; and
- the effectiveness of the security measures deployed should be regularly tested, assessed and validated.

WHO DO I NEED TO NOTIFY IF THERE IS A DATA BREACH?

A significant change introduced by GDPR is the requirement for mandatory notification of personal data breaches in certain circumstances.

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. In short, it is a type of security incident involving personal data.

The key points on reporting may be summarised as:

- If there is a personal data breach, you must notify the ICO without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach.
- The ICO need not be notified, however, if an objective assessment determines that the breach is unlikely to result in harm to individual data subjects.
- If there is a high risk of harm to individuals, there will be an obligation to notify them personally.
- All data breaches should be recorded in a data breach register; regardless of whether or not the breach is notified to the ICO or the individuals.

Security incidents do not necessarily just occur during business hours and procedures within the firm should ensure that there is an ability to move quickly following an incident. The speed of response can be crucial in terms of containing incidents, recovering personal data and taking steps to mitigate any harmful impacts on the affected individual data subjects. Were a breach to occur on Friday evening, the damage could be irreparable by Monday morning.

ACTION

Establish procedures to deal with personal data breaches.

Provide training to employees and contractors to ensure that they can recognise data breaches, and respond appropriately.

Create a personal data breach register and record all personal data breaches, whether notified or not.

If you determine not to notify the ICO or individuals about a breach, keep a record of your reasons and make sure these reasons are legitimate.

FURTHER READING

WP29 – Guidelines on personal data breach notification (see WP29 website)

WHAT RIGHTS DO INDIVIDUALS HAVE IN RESPECT OF THEIR DATA?

GDPR enhances many of the existing rights of individual data subjects and introduces some new ones. The main rights are summarised briefly below.

SUBJECT ACCESS – individuals have a right to request copies of their personal data and to receive further information about the processing of their data.

CORRECTION – individuals have the right to require correction of any personal data which is inaccurate, incomplete or not up to date.

DELETION – individuals can require that their personal data be deleted in certain circumstances.

OBJECTION – individuals have an absolute right to stop direct marketing activity and to object to processing on certain other grounds.

PORTABILITY – in certain circumstances individuals have the right to require that data being processed on an automated basis be sent to them or another controller in a commonly used machine readable format.

AUTOMATED PROCESSING – individuals have specific rights to be protected from automated processing of their personal data which result in decisions about them which have legal or other significant implications for them.

CONSENT – where processing of personal data takes place on the basis of consent, individuals can withdraw that consent at any time.

The basic timescale for responding to individual requests is one month, although that period can be extended in certain circumstances. Requests must be responded to free of charge although there are specific provisions giving controllers protection against requests which are 'manifestly unfounded or excessive, in particular because of their repetitive character'.

ACTION

Understand the rights and if/how they apply to the personal data which is processed by the firm.

Review or establish plans and processes to deal with these enhanced/new rights.

Provide employees with training to recognise requests by individuals to exercise their rights and know what to do with them (bearing in mind the importance of meeting timescales).

Develop template response letters.

Develop a procedure and training for those who will be dealing with data subject requests.

Consider whether technology can be developed or deployed to assist in handling requests.

FURTHER READING

WP29 – Guidelines on automated decision-making and profiling

WP29 – Guidelines on the right to data portability

CONCLUSIONS

If you have not already done so, you should give immediate attention to the implications of GDPR for your firm. Reviewing and understanding the issues set out in this Guide will be a good starting point. Completing the GDPR checklist which is associated with this Guide is another way to get moving.

Firms that comply with existing data protection legislation should find that the journey to GDPR compliance is shorter than those who don't. Either way, the best way to achieve compliance is to try to develop a culture within the firm that understands the importance of protecting the personal data of clients. Thankfully, there is a lot of publicly available information to help CAs to understand what will be required of their firms and we hope that this Guide is a useful contribution to that body of material.

LIST OF STYLE DOCUMENTS

(i) GDPR checklist

(ii) Style clause for letter of engagement

(iii) Style clause for commercial contract

(iv) Style privacy notice – external

(v) Style privacy notice – internal

(vi) Style data processing register

CA House21 Haymarket YardsEdinburghEH12 5BH
enquiries@icas.com+44 (0)131 347 0100 icas.com