MY FIRMS APP™

PREPARING YOUR PRACTICE FOR GDPR

www.myfirmsapp.com>>

ABOUT MYFIRMSAPP

MyFirmsApp develops compliant, personalised Apps with a wide range of tools that leverage the power of mobile technology and put the accountant right at the centre of the mobile world.

We have developed over 1000 Apps for accountants and bookkeepers that are used by over a quarter of a million businesses daily to manage their finances. You need only to enter the search term 'accountants' in the iOS App Store and the Google Play Store to gain an insight into some of the eye-catching custom branded Apps we have developed for our customers but it is always their names you will see, not ours.

Mobile Apps keep users more engaged and build brand loyalty by providing users with greater functionality, integration, simplicity and utility. Rather than wading through numerous 'best of breed' Apps on their mobile devices, clients can save time by accessing their accounts, finance and tax information and systems through a single App and this helps cement the firm's position as its clients' trusted and most authoritative anchor point in the mobile world. Embracing digital mobile will ensure a connection when and where it matters.

While the UK remains our largest market with 30 of the top 100 UK accountancy practices running Apps developed by us, the global market is growing rapidly too and our Apps are now used in nine countries including Australia and the U.S. where MyFirmsApp was named best new Online App in 2017 by the respected publication, Accounting Today.

Every single App developed is of the highest quality, fully endorsed and compliant with industry professional bodies and is constantly updated to include the latest technology so practices save time and money. Working in partnership with our customers, partners, and major drivers in the industry, such as Apple, the goal is to develop solutions that work with its' strict new rules and regulations and continually push innovation forward.

Our priority is putting accountants first and helping guide them into the digital world. MyFirmsApp is the only company to offer 24-hour on-going support, backed by the wealth of experience that comes from running the largest global customer App platform in the world for accountants in practice. We do this thanks to a highly talented, dedicated and passionate team, who are all part of the MyFirmsApp family.

CONTENTS

4 Preparing for GDPR – Revolution not evolution

5 What is GDPR?

5 What type of data does a practice typically hold?

6 Data retention

7 GDPR and MTD - a natural marriage

8 What are controllers and processors?

9 Records of data processing activity

10 Individual rights

10 Data security and breaches

11 Consent

12 How does your own App simplify GDPR?

15 Things to be done

16 Free Download / Suppliers

This guide is intended to provide practical insight on what to do now to prepare for the new legislation and it is not intended as definitive guidance on all aspects of the GDPR.

PREPARING FOR GDPR EVOLUTION – NOT REVOLUTION

UK Business is braced for yet another challenging year ahead of legislative change with the Data Protection Bill, which will transpose General Data Protection Regulation (GDPR) and become UK law on the 25th May 2018. Its' aim is to harmonise data protection laws across Europe and replace out of date legislation that makes no allowance for the way in which data is now collected.

Smartphones, social media and other new digital technologies have transformed the data collection process and with more types and greater volumes of data anticipated in coming years, enhanced security is a necessity.

Although the Information Commissioner has called GDPR a 'game changer', personally I prefer to believe it is more 'evolution' than 'revolution' and as your firm will already be registered with the ICO and compliant with the current law, then that is a good starting point to build on. If your firm hasn't yet started preparing for GDPR, then kick-start the process by mapping out all the data the firm holds to discover exactly what this information is, how it is stored and who it is being shared with.

Over the last year, we have been working closely with selected global law firms and advisors to find solutions to the GDPR challenges faced by our customers and are confident that having a custom branded App will help in the collection and verification of data, in gaining the necessary opt in permissions, in the sharing of privacy policies and also in the storage and management of data. GDPR presents an opportunity to revise existing privacy policies and achieve better organisation, improve data management and strengthen defences against data breaches and cyber risks.

Apps have become an increasingly critical channel for virtually all consumer businesses in all industries and mobile is undeniably now the first screen with each user spending nearly 1.5 months in Apps per year. Despite irrefutable evidence that Apps are here to stay; the question is still asked; 'Will my client use an App?' Our response is always 'It's your clients that are driving the demand for easier engagement through Apps.'

New advances in App-driven technology are being used to power day-to-day processes in accountancy practices and helping to solve compliance challenges. We hope you will find this guide useful and that you will give us the opportunity to demonstrate how the App solution simplifies GDPR, compliance, data collection and more – we can do this by setting up a free demonstration for you and your team (see page 15).

As with all compliance challenges, there can be an easier way.

J. Oliver

Joel Oliver | CEO | MyFirmsApp | joelo@myfirmsapp.com

[1] App Annie

WHAT GDPR MEANS TO YOUR PRACTICE

What is GDPR?

The EU General Data Protection Regulation (GDPR) comes into force on May 25th 2018 and replaces the 1995 Data Protection Directive. It is directly applicable in all EU member states and will apply in the UK despite Brexit. It will affect all businesses that process (i.e. collect, record, use or disclose) data relating to an identified or identifiable natural person ("personal data") and is an attempt to harmonise data protection laws. While many key principles and concepts remain the same, there are several new prescriptive requirements and those found to be non compliant, could face fines of up to 20m euros or 4% of annual turnover.

What type of personal data does a practice typically hold?

The new requirement for transparency means firms need to be open about how they process personal data. Privacy notices must be shared with all individuals you process personal data about and in essence, should include informing those individuals what information you hold on them, how you use it and who you share it with. The most prominent new requirement is that privacy notices must detail the legal bases of processing (e.g. consent, necessary for performance of a contract, legitimate interests). For most firms, this will mean that existing privacy notices will need to be reviewed and updated and the information in them must be concise, transparent, intelligible and easily accessible.

Here are some examples of personal data typically held by accountants:

HR data (current/former staff, applicants, dependants):

- Contact details (e.g. address, phone number)
- Financial information (e.g. salary, tax codes)
- Recruitment information (e.g. CV, application form)
- Admin data (e.g. absence records, hours worked)
- Whereabouts (e.g. electronic card access systems)
- Data re use of assets (e.g. computers, telephones)
- Performance data (e.g. appraisals and disciplinaries)
- Benefits data (e.g. health insurance, pension)

Client data

- Contact details (names, email addresses etc)
- Records of customer interactions
- Payment details
- Online identifiers, IP addresses, cookie IDs
- Profile data (preferences, interests, browsing history)

Business data (suppliers, agents, contractors):

- Contact details (names, email addresses etc.
- Records of customer/supplier interactions
- B2B CRM data

Data from children

For those practices that hold children's personal data, special care is needed, as GDPR requires parental consent for processing children's personal data. Controllers should obtain the consent of a parent or guardian when processing the personal data of a child under the age of 16 and they also must make "reasonable efforts" to verify that a parent or guardian has provided the appropriate consent.

Supplier contracts

With GDPR, additional mandatory clauses in supplier contracts are needed and terms are much more detailed. All existing contracts will need to be reviewed, prioritised and amended to ensure all elements are present and any contracts in place on the 25th May 2018 will need to meet the GDPR requirements. A possible solution would be to send an addendum to existing suppliers and for new suppliers, review template contracts to ensure GDPR requirements are included.

What does the law require with regard to data retention?

GDPR builds on and adds further detail to existing Data Protection Principles and the law requires firms:

1. Process personal data lawfully, fairly and in a transparent manner
2. Collect personal data only for specified, explicit and legitimate purposes
3. Ensure personal data is adequate, relevant and limited to what is necessary
4. Ensure that personal data is accurate and up to date
5. Do not store personal data for longer than necessary
6. Ensure appropriate security for personal data
7. To appoint a data protection officer for certain types of organisation
8. Ensure policies/procedures are proportionate to controller's business and risks
9. Maintain appropriate records to demonstrate compliance

GDPR and Making Tax Digital – a natural marriage

What have GDPR and Making Tax Digital got in common? From the accountant's perspective, it is all about the collection of data in a digital format and how to resolve the complexities of converting huge volumes of records into a format considered acceptable by HMRC.

To thrive in this digital world, we firmly believe that new approaches and new tools are required. That's why we have developed 'Collect', which forms part of the accountant's own branded App and sits on the client's Smartphone or tablet. It's designed for those clients who are non-VAT registered and employ no staff and may find digital record keeping with standard bookkeeping cloud packages a daunting experience. Collect enables them to enter data using the App and is as easy to use as the social media Apps like Facebook.

Data is collected in real time and it is then up to the accountant to review the figures, approve them and with one click, submit them to HMRC. This is the efficient, GDPR compliant, efficient way to manage clients' MTD affairs.

To arrange your free demonstration of the App with MTDfB Collect Solution, please see page 15.

Next Steps

1. Review the length of time personal data is kept.
2. Consider purpose for which data held.
3. Securely delete/anonymise data that is no longer needed.
4. Put in place appropriate and proportionate data retention policy.

What are controllers and processors?

The GDPR makes it a requirement that organisations appoint a data protection officer (DPO) in some circumstances:

- If a public authority (except for courts acting in their judicial capacity).
- If it carries out large scale systematic monitoring of individuals (for example, online behaviour tracking).
- If it carries out large scale processing of special categories of data or data relating to criminal convictions and offences.

A single data protection officer may be appointed to act for a group of companies or for a group of public authorities, taking into account their structure and size. Any organisation is able to appoint a DPO.

A Controller is 'The natural or legal person, public authority, agency or other body which, alone or jointly with others determines the purposes and means of the processing of personal data' (Art 4(7) GDPR).

Points to note:
Businesses are controllers for HR/Business/Consumer data.
Controller has overarching responsibility.
Service providers are generally clients' 'processors'.

A Processor is 'The natural or legal person, public authority agency or other body which processes personal data on behalf of the controller (Art 4(8) GDPR).

Points to note:
Service providers are normally processors but can be controllers if use data for own purposes.
Service providers will be both controllers and processor for different types of data.
GDPR imposes some direct liability on processors.

Records of data processing activity

The law requires:

- Maintenance of internal records of data processing activities (if >250 employees or "higher risk" processing etc.).
- Records must include range of information in the GDPR (e.g. purposes of processing, data categories, recipients, data retention periods, security measures).
- ICO can request the records at any time.

Accountancy practices should undertake a detailed review of their personal data processing activities and should assess the legal basis for processing personal data (e.g. consent, legitimate interest, compliance with law or to perform a contract) and keep a record of the basis. Firms relying on consent from individuals to process their personal data will need to meet the new, higher standard requiring consent to be informed, specific, freely given, unambiguous and revocable. Pre-ticked boxes, silence or inactivity will not meet the new standard. Accordingly, firms should review client care letters and marketing materials and, where appropriate, ensure consent is renewed.

Next Steps

Consider how client consent was given for processing purposes and recognise that pre-ticked boxes or silence will no longer constitute consent. Look at preparing new standard templates to obtain consent for marketing purposes, which clearly explain how the data will be used and for how long it will be stored.

1. Implement an internal record of data processing activities.
2. Document what personal data is held, where it came from and who it's shared with.
3. Take advantage of existing HR systems and databases.
4. Depending on volume and complexity of data processing, consider carrying out a data audit.

Individual rights

GDPR builds on and expands individuals' existing rights and introduces some new rights. Notably, the firm cannot refuse or charge for complying with rights requests unless manifestly unfounded or excessive and requests must be handled within one month – this can be extended up to two.

1. The rights of access and data portability
2. The right to rectification
3. The right to erasure
4. The rights to object and/or to restrict processing
5. Rights in relation to certain solely automated decisions

Next steps

1. Check procedures and determine how you would respond if request is made
2. Consider whether need to revise procedures and make any changes
3. Analyse whether systems are able to locate specific personal data and delete or anonymise it
4. If there are no policies, create, implement and periodically review and train staff

Data security and breaches

What is a data breach?

An incident leading to destruction, loss, alteration, unauthorised disclosure of, or access to personal data and this is more than the loss of personal data or getting hacked, it includes where data is sent to the wrong recipient. Controllers must notify the ICO within 72 hours of becoming aware of a data breach and in some cases, individuals. According to a recent study data breaches in the financial services sector increased 937% year-on-year from 2015 to 2016 so it is vital that practices review their existing IT security measures and check whether they meet the highest security settings of "data protection by design and default" which the GDPR requires for personal data. Any breach caused by human error or lax security measures threatens the accountant client relationship.

Practices need to ensure they have the technologies and processes in place that will enable them to detect and respond to a data breach. This will undoubtedly involve changes to internal data security policies and these will need to be clearly communicated to staff with additional training to ensure data breaches are properly understood and can be easily recognised.

Next steps

1. Check procedures and determine how a data breach would be handled
2. Given timescales for reporting, it is important to have robust detection investigation and internal reporting
3. Policies must be implemented – relevant personnel must be trained and required to comply
4. Staff must understand what constitutes a data breach and that this is more than just loss of personal data

[2] IBM X-Force Research Team

CONSENT

What the law requires

- Consent must be freely given, specific, granular, informed and unambiguous indication of wishes
- Clear affirmative action which is essentially a positive opt in and consent cannot be inferred from silence or pre-ticked boxes
- Consent must be verifiable e.g. time stamped records in a CRM database
- Consent wording and mechanisms must be separate and prominent from other T & Cs
- Simple ways to withdraw consent at any time

Next steps

While GDPR does not specifically require to automatically refresh all consents under current law, review how the practice seeks, records and manages consent particularly for direct marketing.

For certain marketing, which does require consent, consents may need to be refreshed if not GDPR compliant and ensure any re-permissioning is approached carefully.

Data Protection Impact Assessments (DPIAs)

DPIAs are mandatory where data processing is likely to result in high risk to individuals such as in deploying new technology, sensitive profiling activities and in the large-scale processing of sensitive data and they must be recorded and documented in a specific way.

The ICO must be consulted if DPIA indicates data processing is high risk and the risks are not sufficiently mitigated.

HOW AN APP SIMPLIFIES AND AIDS GDPR COMPLIANCE

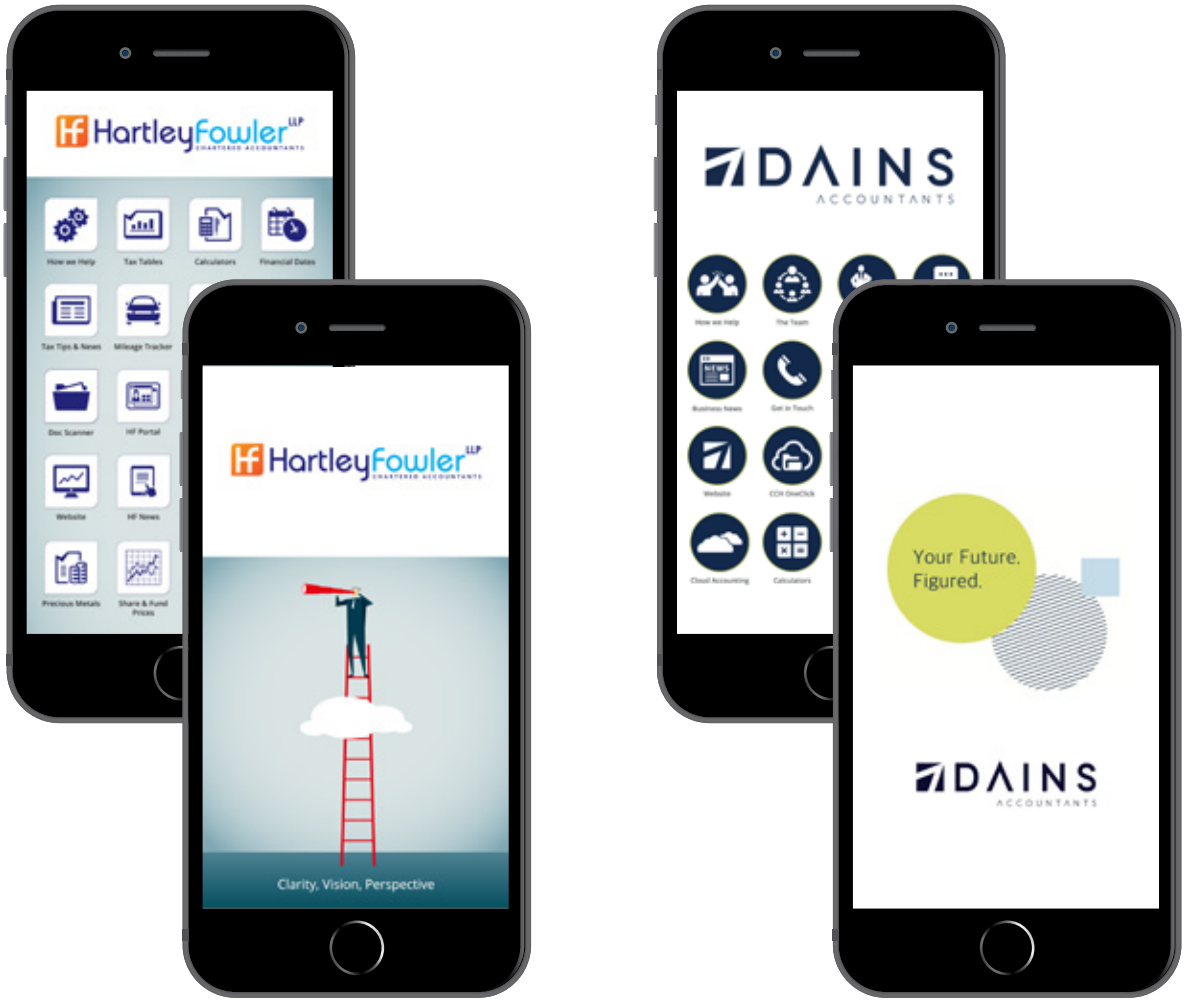
Apps have become an increasingly critical channel for virtually all consumer businesses and mobile is now the first screen and the primary touch point, just like websites once were.

In today's 24/7 mobile world, the accountant's position as the first point of contact to discuss financial issues, is being challenged as pressure to do more with fewer resources nudges clients and prospects down the quickest and easiest route to information on accounts, finance and tax. By delivering access to this valuable information directly to the client through a custom, branded App, accountants can neutralise threats such as 'the Google effect' and cement the firm's position as its' clients' trusted anchor point in the mobile world.

Today's Apps do so much more than just connect accountants with their clients. They are comparable to integrated suites of practice software that roll up tools, features and content and make the practice more efficient.

Delivering a solution that aids GDPR compliance is a natural next stage for the App platform and we are working closely with selected global law firms to ensure the newly developed OneApp platform performs this vital role in collecting and verifying data, gaining opt in permissions, sharing privacy policies and in storing and managing key data in a compliant and user-friendly manner.

The contact data, and segmentation held in the accountant's App control panel, is totally secure and access can be restricted to selected members of the team. If a user wishes to be 'forgotten' then they can simply delete the App from their device and notify the practice that they do not wish to be contacted again. All their contact information can be easily removed from the control panel and a complete audit trail is available to demonstrate these actions have been completed.



Secure, effective and compliant client communication

Apps can be used to send messages to clients very effectively and with a 90% open rate compared with emails that have an open rate of around 4%. Push notifications are short, text like messages, which are sent instantly and automatically land on all App users' phones or tablets. The beauty of this method is that most people have their phones with them all the time and messages don't have to fight for visibility with hundreds of other emails in a crammed-full inbox or a pile of junk mail carefully filtered by a secretary or PA.

Furthermore, they provide a helpful, additional layer of protection and ensure any information relayed is totally secure.

As the App inherently works on an 'opt-in' basis, clients have to choose to download it and this opt-in theme continues with an option to receive push notifications. Push notifications can also be segmented so that relevant messages are sent to selected prospects and clients and those that download the App are given the choice of opting-out of certain preferences.
Those practices that have an App developed by us can enjoy deep levels of integration with partner, Reckon, who has developed a secure electronic document management portal that encrypts and secures every document going back and forward between the accountant and the client. Use of a portal guarantees complete security and traceability through a full audit trail and allows users to publish documents to an individual notifying them via an email address.

Data gathering for MTD

While communication is an important part of the new GDPR landscape, how accountants gather their clients' data is set to take on even more prominence as we move towards the introduction of 'Making Tax Digital for Business'.

Accountants tell us that they are most concerned about their smallest clients; the ones that still bring their records into the office in shoeboxes and keep notebooks. For this group, the new digital landscape represents a sea change in the way they manage their finances and it is down to the accountant to consider how best to help them make this transition to digital record keeping and start preparing them now. The key advantage is that a switch to digital technology enables the accountant to look at clients' live records electronically and to give prompts and advice in a way that is simply not possible when the business keeps handwritten records.

Any mention of electronic data collection and record keeping can create panic and there needs to be a simple answer to the recurring and unprofitable challenge of getting information from clients that want to use their Smartphones to communicate with their accountant. The solution lies in the newly developed, easy to use 'Collect' App that is ideally suited to recording simple transactional data.

By providing business clients with a single simple App, they can collect the information needed by using the in-built camera on their Smartphones and Tablets to photograph receipts and by taking photographs of their invoices. Traditionally, getting the data to the accountant has involved manual exports of that data from the App itself but a Cloud portal changes this by allowing the accountant to login directly and gain instant access to any information collected by their client including income, expenditure and mileage logs.

There is a compelling opportunity for all firms, large and small, to reboot their data protection and privacy processes and turn to digital technology to prepare for GDPR and MTD. An inclusive, compliant App platform that reflects the importance the firm places on privacy, will deepen digital trust, make clients feel more secure when they give their personal data to the firm and help enhance the practice's reputation.

Download the world leading accountancy App today and see how it could benefit your firm and your clients.
Visit www.myfirmsapp.co.uk

THINGS TO BE DONE

- [ ] Arrange your free demonstration of the App (see page 15).
- [ ] Appoint an overseer of the process.
- [ ] Review IT processes and whether communication is secure.
- [ ] Document the data held by the practice.
- [ ] Review contracts with clients, suppliers and employees.
- [ ] Draw up data protection policies and procedures.
- [ ] Review consent processes.
- [ ] Identify what to do if there is a data breach.
- [ ] Consider data collection, storage, permission.
- [ ] Importance of the right to remove.
- [ ] Privacy Policy.
- [ ] Train staff.

FREE DOWNLOAD AND 1:1 WALKTHROUGH

Download the world leading accountancy App today and see how it could benefit your firm and your clients.

Once you have downloaded the App, we will contact you to arrange your FREE 1:1 walkthrough. This is your exclusive opportunity to talk to one of our mobile experts, 1:1 via phone or Skype. It's a rare opportunity for you to see how firms like yours are using this new technology to get connected and importantly why they love it. You'll also discover what return on investment you can expect and critically how it will work for your business.

During your call you will also hear for yourself why it's so popular – nominated as Top Mobile Product by Accounting Today and why it produces comments like "It's one of the most exciting things I have seen in 25 years of accounting!"

SUPPLIERS

RAY LEVY LAW OFFICES

RAY LEVEY

RAY@RAYLEVYLAW.COM

0203 6968920

We've used Ray for multiple projects, he is fantastic at drafting policies, terms and conditions, disclaimers etc.

LAUGHLIN CONSULTANCY

PAUL LAUGHLIN

PAUL@LAUGHLINCONSULTANCY.COM

07446 958061

We've used Paul to help complete a GDPR audit of the business, work with us to implement solutions and ensure that the services we provide are GDPR compliant.

GREGG LATCHAMS SOLICITORS

ED BOAL - SENIOR ASSOCIATE

EDWARD.BOAL@GREGGLATCHAMS.COM

0117 9069 486

We've worked with Ed to review the processes we were implementing and the customer Journey.

CLIENT COMMENTS

"I would like to personally thank you for spending almost 3hrs with me on the phone today exploring, explaining, and overviewing nothing short of every aspect of both the dashboard as well as the App itself. We have undergone many technology upgrades lately and it is great to know that we have a strong, knowledgeable, and easily approachable support base that has given us the added confidence we needed with this project."

Mark Carbone ~ Tilenni Stiles

"We have been using it for about a year now The Receipt Manager is the most used page and we also promote it regularly in our e-newsletter and the articles about it are consistently opened and read. I personally love it. It's such a unique talking point. When I tell someone we have an app, they're always very impressed and think it's exceptionally cutting edge."

Stephanie Chapa ~ Wiebe Hinton Hambalek, LLP

"We subscribed to MyFirmsApp after being impressed at Accountex 2015. The implementation was smooth and the functionality has raised our profile with clients, providing them with useful tools to enhance decision making and controls"

Stephen Farra ~ Stephen Farra Associates

MY FIRMS APP™

PREPARING YOUR PRACTICE FOR GDPR

www.myfirmsapp.com>>

CONTACT WITH US

UK
37-39 Victoria Road,
Darlington,
Co. Durham,
DL1 5SF

contact@myfirmsapp.com
0800 803 0826

Global
+44 (0)1325 469 603

Australia
02 8015 5480

USA
347 748 9098