GDPR FACTSHEET

What is GDPR?

GDPR stands for General Data Protection Regulation; it's a piece of legislation which will significantly change and update the data protection regime across the entire European Union. GDPR has come about in part to gain control over the way in which some of the large global organisations such as Facebook and Google store and handle personal data, as well as to harmonise regulations across EU countries.

KEY ISSUES

GDPR makes existing Data Protection rules more stringent.

Data subjects (individuals about who personal data is collected, stored or processed have more rights and data processors (organisations) have more responsibilities.

Fines for breaching the new rules can run to many £millions.

GDPR comes into force on 25 May 2018, and organisations need to act now to ensure they are ready.

What's changing?

GDPR brings in more stringent controls on processing personal data generally. In particular, data subjects are given more information about use of their data including:

- exactly what data they are collecting
- what it will be used for, and
- how long it will be kept

GDPR also expands the definition of personal information to include new types of data:

- Actions/behaviour (such as that tracked on website analytics)
- IP address
- Job title

GDPR also gives data subjects more rights to erase, correct and see their own personal data and makes it a requirement that specific consent to marketing is on an 'opt-in' rather than 'opt-out basis. It also introduces new reporting requirements for data protection breaches and new processes including Privacy Impact Assessments & Data Protection by Design.

What do I need to do?

If you're in charge of compliance for an organisation:

Most organisations will already be subject to data protection rules, and those in financial services will be used to complying with quite strict regulations and will have the foundations of GDPR compliance already in place. Others will be starting more or less from scratch, and for small businesses this could seem like a fairly daunting task. There is a wealth of information on the Information Commissioner's Office (ICO) website and if you're a member of a trade body or association they may be able to provide some guidance specific to your area of work. The ICO suggests 12 steps which provide a useful starting point.

As an individual:

You'll start to notice the companies and websites you engage with asking you to update your consent or permissions. They may also change terms and conditions and service agreements to reflect the changes the new rules require. The good news is that the new rules should result in a lot less junk mail in your inbox as only those organisations to whom you've given specific consent can market to you.

GDPR and working with Aspira

Aspira takes data protection very seriously and has always been subject to the UK's current Data Protection rules. As a result we've always had a Data Protection Officer (Andy Chidgey) who oversees compliance with these regulations. We have a written Security Policy which is checked and audited on an annual basis and which all employees must adhere to. The Security Policy details the way in which Aspira stores and processes client data, and all our processes and procedures are set up accordingly.

GDPR comes into force on 25th May 2018 and we have a project team working on making the small changes required to comply with the new rules. Keep an eye on our website and Twitter account for updates. In the meantime we will be carrying on business as usual.

GDPR Factsheet (FS GDPR 01 2018) written by Aspira.
Registered office Manor Farm, Aust, Bristol, BS35 4AT.
Aspira is a trading name of Aspira Corporate Solutions Limited which is authorised and regulated by the Financial Conduct Authority.
Aspira Corporate Solutions Limited registered in England no: 7839452.

GDPR FACTSHEET

Frequently Asked Questions:

Q. I'm an employer, can I still share information about my employees with you?

A. If there is a signed service agreement with Aspira and we are contracted to provide an advice service to your employees it is lawful for you to send us their personal data. We still need you to do this so that we can perform services in accordance with our contract with you.

Q. I want to opt out of your email newsletter, can I do this?

A. While you are free to unsubscribe from our regular newsletter at any time we should point out that they form part of our ongoing service to you. They are there to provide you with important information about your plans, your options and our service.

Q. What changes might I notice from Aspira?

A. You will see the consent wordings become more specific as we include more detail about exactly what information we keep, how long we store it and how we use it. These changes will happen in the run up to May 2018.

Q. I don't have / don't want to provide an email address, will this be a problem?

A. We use a system called the Personal Finance Portal (PFP) which works in a similar way to online banking and requires a personal email address. It allows us to communicate with you securely via a messaging system and also enables both us and you to share and store important financial documents in a secure environment. If you don't have an email address you will not be able to use the PFP.

Q. Who will my information be shared with?

A. We have strict processes for data security and we will only share your data where absolutely necessary in order to fulfil our service. Clearly we will need to share personal data with product providers in order to set up, administer and review your individual plans. They are also obliged to comply with GDPR and will we will also have completed our due diligence process to satisfy ourselves that third parties are operating within the law.

12 STEPS TO GDPR COMPLIANCE

1. Awareness
Are all the key stakeholders in the organisation aware of the changes and their impact? Have all areas that could cause issues been identified?

2. Information you hold
Have you documented what personal data you hold, its origin and who it is shared with?

3. Communicating privacy information
Have you documented your legal basis for processing personal data, the retention periods and the complaints process?

4. Individual rights
Is everyone aware of the individual's rights regarding their personal data (e.g. accuracy, rectification, erasure etc.)?

5. Subject access requests
Do you have a documented process for responding to a subject access request, in accordance with GDPR?

6. Legal basis for processing data
Have you established & documented your legal basis for data processing?

7. Consent
Do your current consent wordings comply with GDPR? If they need updating how will this be achieved?

8. Children
Do you have a documented policy for dealing with children?

9. Data breaches
Do you have a clear understanding of breach notification rules and a documented breach notification process?

10. Data protection by design
Are projects processes undertaking with data protection in mind at design stage? Do you understand what a data protection impact statement entails and when it's needed?

11. Data protection officer
Do you have a designated data protection officer who'll be responsible for general oversight?

12. International
Do you operate across more than one EU member state? If so you may need to identity and document your lead data protection supervisory authority (e.g. Information Commissioner's Office in UK).

GDPR Factsheet (FS GDPR 01 2018) written by Aspira.
Registered office Manor Farm, Aust, Bristol, BS35 4AT.
Aspira is a trading name of Aspira Corporate Solutions Limited which is authorised and regulated by the Financial Conduct Authority.
Aspira Corporate Solutions Limited registered in England no: 7839452.