A GUIDE TO EU GENERAL DATA PROTECTION REGULATION (GDPR)

FIRST SOLUTION
IT SUPPORT & CYBER SECURITY

A GUIDE TO EU GENERAL DATA PROTECTION REGULATION (GDPR)

Congratulations! If you're reading this guide then you've probably just been promoted to Data Protection Officer for your company. This guide is intended for people who have are professionally involved with the responsibility for complying with the EU General Data Protection Regulation (GDPR). We wrote this guide to help you form a GDPR compliance strategy. As IT experts even we find it confusing when searching the Internet for GDPR solutions providers. It's so confusing because so many IT companies are positioning themselves as GDPR experts with the aim of selling products and services. They appear to focus on listing product and platform features and types of service which often make no sense to those in a Data Protection Officer role.

We wrote this helpful guide to help people like you undertand the right direction of travel based on criteria we know to be important to your role, such as;

How choosing the right GDPR solution provider can help minimise costs and risk to your business.

How the right GDPR solution provider can help you to unlock innovation and provide better service to your customers and free up valuable resources for more important tasks like driving growth.

But first things first "who are you and why are you writing this guide?" and "what's in it for both of us?"

WHO ARE WE?

We're First Solution Technologies Limited, and since 2005 we've provided a mix of IT consulting and cloud solutions to help clients realise their desired business outcomes through the effective use of technology. Err, hang on a second - we've just committed the cardinal sin that all IT support companies do. We've immediately lapsed into 'geek speak'. So, here's the deal – whenever we lapse into geek speak you'll see this icon…

…and whenever you see it please refer to the handy alphabetical glossary at the back of this guide or on our website which will explain the term cloud solutions further. All throughout this guide we're going to talk to the lowest common denominator and provide further explanations where necessary by pointing you to our website or blog articles using this icon…

…for more detail. Our goal is to equip you with the best advice and tactics that empower you to make the best decisions for your business when choosing a GDPR solutions provider.

Montpellier House, Montpellier Drive, Cheltenham, GL50 1TY
Tel: 01242 335549 | email: info@firstsolution.co.uk | www.firstsolution.co.uk
Company Registration: 04491556 | VAT Registration: GB 798 1835 68

FIRST SOLUTION
IT SUPPORT & CYBER SECURITY

WHAT'S IN IT FOR US?

We want you to be happy, in fact we really want you to be delighted. We've found that delighted people promote our business which creates customers and is a virtuous circle. We want you to find the answers you're looking for right here in this guide or on our website. We are so obsessed with creating delighted customers it is at the heart of everything we do. By being very easy to deal with, highly professional and pleasant to be around we hope that you'll keep coming back to us for information. And once you keep coming back to us it's just a matter of time before you get in touch (and we'd love you to do that by the way so don't be shy). Therefore, we've created this guide with you in mind and given it away for free as proof of our desire to educate, support and empower people just like you. Now, that's enough of that touchy-feely stuff so let's gets right into why you're here.

WHAT'S IN IT FOR YOU?

We can guess that as you're reading this guide that you probably work in a compliance role, or have been tasked with leading your companies GDPR compliance efforts. You're may also be looking for help implementing a GDPR compliance strategy that probably means that you may be involved with your company's IT support decision making as the two areas of expertise are closely intertwined, preventing data breaches is the most common example. Our aim is to equip you with the knowledge that you need to to ensure your business is GDPR compliant, using your existing IT support infrastructure wherever possible.

Montpellier House, Montpellier Drive, Cheltenham, GL50 1TY
Tel: 01242 335549 | email: info@firstsolution.co.uk | www.firstsolution.co.uk
Company Registration: 04491556 | VAT Registration: GB 798 1835 68

FIRST SOLUTION
IT SUPPORT & CYBER SECURITY

12 STEPS TO TAKE NOW

This checklist highlights 12 steps you can take now to prepare for the General Data Protection Regulation (GDPR) which will apply from 25 May 2018.

1. *Awareness:* You should make sure that decision makers and key people in your organisation are aware that the law is changing to the EU's GDPR on 25th May 2018. You need to understand the impact this is likely to have.
2. *Information you hold*: You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit which we would be delighted to help you with.
3. *Communicating privacy information*: You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation. For example, does your website contain a privacy page?
4. *Individuals' rights*: You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
5. *Subject access requests:* You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.
6. *Lawful basis for processing personal data:* You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.
7. *Consent:* You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.
8. *Children:* You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.
9. *Data breaches:* You should make sure you have the right procedures in place to detect, report and investigate a personal data breach. At First Solution, we can help advise on the suitability of your data breach procedures and ensure fitness for purpose.
10. *Data Protection by Design and Data Protection Impact Assessments:* You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation. You may need to organise an Privacy Impact Assessment for your business which we would be delighted to help you with.
11. *Data Protection Officers:* You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer. At First Solution we can act as a Data Protection Advisor for your business.
12. *International:* If your organisation operates in more than one EU member state (i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

Montpellier House, Montpellier Drive, Cheltenham, GL50 1TY
Tel: 01242 335549 | email: info@firstsolution.co.uk | www.firstsolution.co.uk
Company Registration: 04491556 | VAT Registration: GB 798 1835 68

FIRST SOLUTION
IT SUPPORT & CYBER SECURITY

INTRODUCTION

The s main concepts and principles of GDPR are much the same as those in the current Data Protection Act (DPA), so if you are complying properly with the current law then most of your approach to compliance will remain valid under the GDPR. There are new elements and significant enhancements, so you will have to do some things for the first time and some things differently.

Use this checklist and other resources to work out the main differences between the current law and the GDPR. It is essential to plan your approach to GDPR compliance now and to gain 'buy in' from key people in your organisation. You may need, for example, to put new procedures in place to deal with the GDPR's new transparency and individuals' rights provisions. In a large or complex business, this could have significant budgetary, IT, personnel, governance and communications implications.

The GDPR places greater emphasis on the documentation that data controllers must keep demonstrating their accountability. Compliance with all the areas listed in this guide will require organisations to review their approach to governance and how they manage data protection as a corporate issue.

Certain elements of the GDPR will have more of an impact on some organisations than on others (for example, the provisions relating to profiling or children's data), so it would be useful to map out which parts of the GDPR will have the greatest impact on your business model and give those areas due prominence in your planning process.

If advice or guidance is sought for how to implement the GDPR within your business then get in touch and we'd be delighted to assist wherever we can.

Montpellier House, Montpellier Drive, Cheltenham, GL50 1TY
Tel: 01242 335549 | email: info@firstsolution.co.uk | www.firstsolution.co.uk
Company Registration: 04491556 | VAT Registration: GB 798 1835 68

FIRST SOLUTION
IT SUPPORT & CYBER SECURITY

HOW TO IMPLEMENT A GDPR STRATEGY WITHIN YOUR BUSINESS

1. AWARENESS

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR on the 25th May 2018. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation's risk register, if you have one.

Implementing the GDPR could have significant resource implications, especially for larger and more complex organisations. You may find compliance difficult if you leave your preparations until the last minute.

2. INFORMATION YOU HOLD

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit across the organisation or within business areas.

The GDPR requires you to maintain records of your processing activities. It updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You won't be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

3. COMMUNICATING PRIVACY INFORMATION

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

When you collect personal data you currently must give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language.

4. INDIVIDUALS' RIGHTS

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format. The GDPR includes the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing

Montpellier House, Montpellier Drive, Cheltenham, GL50 1TY
Tel: 01242 335549 | email: info@firstsolution.co.uk | www.firstsolution.co.uk
Company Registration: 04491556 | VAT Registration: GB 798 1835 68

- The right to data portability
- The right to object
- The right not to be subject to automated decision-making including profiling.

Overall, the rights individuals will enjoy under the GDPR are the same as those under the Data Protection Act but with some significant enhancements. If you are geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy. This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who will make the decisions about deletion? The right to data portability is new. It only applies:

- To personal data an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means.

You should consider whether you need to revise your procedures and make any changes. You will need to provide the personal data in a structured commonly used and machine-readable form and provide the information free of charge.

5. SUBJECT ACCESS REQUESTS

You should update your procedures and plan how you will handle requests to take account of the new rules:

- In most cases you will not be able to charge for complying with a request.
- You will have a month to comply, rather than the current 40 days.
- You can refuse or charge for requests that are manifestly unfounded or excessive.
- If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.

If your organisation handles many access requests, consider the logistical implications of having to deal with requests more quickly. You could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.

6. LAWFUL BASIS FOR PROCESSING PERSONAL DATA

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

Many organisations will not have thought about their lawful basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing.

You will also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request. The lawful bases in the GDPR are broadly the same as the conditions for processing in the Data Protection Act. It should be possible to review the types of processing activities

Montpellier House, Montpellier Drive, Cheltenham, GL50 1TY
Tel: 01242 335549 | email: info@firstsolution.co.uk | www.firstsolution.co.uk
Company Registration: 04491556 | VAT Registration: GB 798 1835 68

you carry out and to identify your lawful basis for doing so. You should document your lawful bases to help you comply with the GDPR's 'accountability' requirements.

7. CONSENT

This is perhaps the biggest and most impactful area of change under GDPR. You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard. Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent. Public authorities and employers will need to take care. Consent must be verifiable and individuals generally have more rights where you rely on consent to process their data.

You are not required to automatically 'repaper' or refresh all existing Data Protection Act consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

8. CHILDREN

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services ('information society services') to children and relies on consent to collect information about them, then you may need a parent or guardian's consent to process their personal data lawfully. The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 here in the UK). If a child is younger then you will need to get consent from a person holding 'parental responsibility'. This could have significant implications if your organisation offers online services to children and collects their personal data. Remember that consent must be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand.

9. DATA BREACHES

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Some organisations are already required to notify the ICO (and possibly some other bodies) when they suffer a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. You only should notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Montpellier House, Montpellier Drive, Cheltenham, GL50 1TY
Tel: 01242 335549 | email: info@firstsolution.co.uk | www.firstsolution.co.uk
Company Registration: 04491556 | VAT Registration: GB 798 1835 68

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.

You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine of up to EURO20,000,000 or 4% of group annual global turnover, as well as a fine for the breach itself.

10. DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- Where a new technology is being deployed
- Where a profiling operation is likely to significantly affect individuals
- Where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

You should therefore start to assess the situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally? At First Solution we can help advise, implement and deliver a DPIA for your organisation, build a risk register or simply provide advice and guidance wherever required.

11. DATA PROTECTION OFFICERS

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

You should consider whether you are required to formally designate a Data Protection Officer (DPO). You must designate a DPO if you are:

- A public authority (except for courts acting in their judicial capacity)
- An organisation that carries out the regular and systematic monitoring of individuals on a large scale
- An organisation that carries out the large-scale processing of special categories of data, such as health records, or information about criminal convictions. The Article 29 Working Party has produced guidance for organisations on the designation, position and tasks of DPOs.

Montpellier House, Montpellier Drive, Cheltenham, GL50 1TY
Tel: 01242 335549 | email: info@firstsolution.co.uk | www.firstsolution.co.uk
Company Registration: 04491556 | VAT Registration: GB 798 1835 68

It is most important that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to carry out their role effectively. At First Solution, we can act as a Data Protection Advisor for your business.

12. INTERNATIONAL

If your organisation operates in more than one EU member state, you should determine your lead data protection supervisory authority and document this.

The lead authority is the supervisory authority in the state where your main establishment is. Your main establishment is the location where your central administration in the EU is or else the location where decisions about the purposes and means of processing are taken and implemented.

This is only relevant where you carry out cross-border processing – i.e. you have establishments in more than one EU member state or you have a single establishment in the EU that carries out processing which substantially affects individuals in other EU states.

If this applies to your organisation, you should map out where your organisation makes its most significant decisions about its processing activities. This will help to determine your 'main establishment' and therefore your lead supervisory authority.

The Article 29 Working Party has produced guidance on identifying a controller or processor's lead supervisory authority.

Montpellier House, Montpellier Drive, Cheltenham, GL50 1TY
Tel: 01242 335549 | email: info@firstsolution.co.uk | www.firstsolution.co.uk
Company Registration: 04491556 | VAT Registration: GB 798 1835 68

FIRST SOLUTION
IT SUPPORT & CYBER SECURITY

THANK YOU

We hope this guide helps in your role and if you have any feedback as to what we can do to improve this guide then please send it with 'FEEDBACK: A guide to EU General Data Protection Regulation' in the subject line to info@firstsolution.co.uk. Thank you for reading and if there's anything we can do to help support and empower you in your role then we'd be delighted to help.

The First Solution Team.

Montpellier House, Montpellier Drive, Cheltenham, GL50 1TY
Tel: 01242 335549 | email: info@firstsolution.co.uk | www.firstsolution.co.uk
Company Registration: 04491556 | VAT Registration: GB 798 1835 68

FIRST SOLUTION
IT SUPPORT & CYBER SECURITY

GLOSSARY

Advanced Machine Learning
Artificial Intelligence
Azure Portal
Before the Gateway
Business Continuity Planning
BYOD
Cloud Based Services
Cloud Desktops
Cloud MSP
Cloud Networks
Cloud Servers
Cloud Solutions
Cloud Solutions Provider
Cloud Telephony
Cyber Essentials
Cyber Security
Cyber Security Audits
Data Analytics
Data Loss Prevention technologies
GDPR
GDPR Preparedness Audit/Independent Audit/Information Audit
Help desk
Internet of Things
Managed Antivirus
Managed Backup and Recovery
Managed Remote Access
Managed Security Services
Managed Services Provider
Managed Web Security
Microsoft Azure
Microsoft Dynamics
Microsoft Office 365
Mobile Device Management
Office 365 Portal
OneDrive for Business
Partner of Record
Patch Management
Proactive IT Support
Reactive IT Support
Remote IT Support
Remote Monitoring and Management
Risk Intelligence Report
Service Delivery Management
Server Cluster
Skype for Business
Software Management
Virtualisation

Montpellier House, Montpellier Drive, Cheltenham, GL50 1TY
Tel: 01242 335549 | email: info@firstsolution.co.uk | www.firstsolution.co.uk
Company Registration: 04491556 | VAT Registration: GB 798 1835 68