GDPR for Small Business

Thomas Hayes
BA Hons, FBCS, CITP, FIP, CIPM, CIPP/E, MAPM

Email: thayes@hayesltd.com

Website; www.hayesltd.com

Contact Telephone: 07834 039328

Hayes Associates offers the following services:

- Data Protection & GDPR Advice
- Data Protection & GDPR Audits
- Cyber Security Audits & Advice
- Data Breach Management
- Subject Access Request Management
- Information Management Consultancy
- Cyber Essentials Accreditation
- ISO 27001 Accreditation
- Data Protection Officer (DPO) as a Service
- Data Protection and Cyber Security Training & Awareness - all staff levels

Introduction

The purpose of this short ebook is to provide an awareness in summary form, of what a small company needs to consider when processing personal data. It summarises the key facts that are salient to your business when considering the rules governing personal data as set out in the General Data Protection Regulation (GDPR).

The use of personal data to undertake your business functions is essential to your ongoing operations. Without data and the associated processing, storage and reporting, there would be no business. As with all things in life – especially for businesses, there are rules that need to be followed. What are these rules?

In this short ebook we shall attempt to explain what GDPR is all about.

What is the General Data Protection Regulation, (GDPR)?

The General Data Protection Regulation, (GDPR), is a Regulation issued by the European Union that formally came into force on 25th May, 2018. The UK Data Protection Act (DPA) of 2018 that incorporates GDPR has replaced its predecessor, the DPA 1998. The GDPR consists of 11 Chapters, 99 Articles and covers 88 pages of text.

This is just the latest in a series of legislation that covers data protection, building on the Data Protection Act of 1998 that preceded the GDPR of 2018. The Data Protection Act is UK law and incorporates GDPR, but also includes other elements either not covered by the EU Regulation or where there is some scope for national level decisions. For example; immigration data and age of children's consent. In essence, the GDPR wasn't a dramatic change from the previous data proaction regime. What generated all of the attention was the level of fines that could be applied – up to 4% of turnover.

Full details can be found here https://gdpr-info.eu

What were the changes brought in by the GDPR?

Despite some focussing of the minds arising purely on the amount of fines that may be levied – anything up to 4% of International or Group turnover, GDPR built upon the previous DPA 1998, it was not a very significant change in the way that the introduction of its predecessor (DPA 1998) was.

The aim of the GDPR is to provide even stronger rights to individuals in dealing with organisations that hold their data. Personal data is defined as anything that may identify a natural person – a living human being. It will include names, identifiers, biometric data, images, and any IP/Internet related data.

There is also a new category of sensitive personal data. This includes; political, religious, Trades Union, philosophical, health and sexual aspects. There is a requirement for some organisations to obtain clear and explicit consent from the Data Subject to process their personal data. Others may use one of the other five lawful bases for processing; contractual obligation, public interest, legal duty, legitimate interest, and vital interest.

Records of this consent must be held where this lawful basis applies, and there is a burden of proof on the Data Processors (Controllers) to show that this remains valid and that its conditions of use are explicitly stated. This means that it cannot be inferred, such as by having a box pre-ticked on a screen. Moreover, the individual also has a further right to withdraw their consent thereafter.

You also need to establish whether you are collecting any children's data. That is, anyone under sixteen years of age for the UK, but can vary by country down to thirteen years. The process needs to be made as easy as possible for the Data Subject to agree consent. The Data Subject is also accorded the 'Right to be Forgotten' – that is, that their data, upon request can be permanently deleted. This is not an absolute right, but will be allowable in many circumstances. In addition, the Data Subject – the person whose personal data is held - has the following rights;

• Enhanced right to information and transparency
• Right of access and rectification
• Right to erasure or "right to be forgotten"
• Right to restriction • Right to data portability

What is Personal Data?

The term ‘personal data’ is defined in Article. 4 (1).

Personal data are any information which are related to an identified or identifiable natural person. The data subjects are identifiable if they can be directly or indirectly identified, especially by reference to an identifier such as a name, an identification number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons

This means that if an individual may be identified through the data that you hold, albeit indirectly, then this counts as personal data. It also only applies to a natural living person and so details about a dead person does not count as personal data.

There are also special categories of personal data - also known as sensitive personal data that are subject to a higher level of protection. These categories of data include; genetic, biometric and health data, as well as personal data revealing racial and ethnic origin, political opinions, religious or ideological convictions or trade union membership.

What are The GDPR Principles?

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

What are the Challenges?

The size of the challenge to organisations is related in proportion to their existing level of compliance with the previous DPA 1998. Being in a good position is a perfect baseline from which to proceed. This position can be measured by the extent of the governance and awareness that is in place, the quality of the record keeping and the maturity of the Information Management and Governance procedures and processes.

Compliance is made easier if all of the above is set alongside the existence of sophisticated IT systems and the appropriate cyber security – all underpinned by a good corporate culture. Change Management must include the data implications. This is essential in order to assess the risks associated. Some of the larger companies have significant problems as they have added products and services over many years, using discrete and individual systems in silos to capture customer details.

They may have also grown their businesses through acquisition (inheriting different systems) and this has resulted in bi-furcated views of their customers. Hence many cannot easily obtain a ‘Single Customer View’. This is particularly the case within Financial Services.

This situation is the result of a rush to market products and services without considering the implications on data. Sometimes this is due to a lack of foresight in information systems strategy. GDPR incorporates the concept of Privacy by Design. This assesses the impact of data privacy by taking this factor into account when designing new systems. This is not a new concept however, and Privacy Impact Assessments have been used in the public sector for some years

What are the Opportunities?

The analogy I like to use for compliance with the GDPR is that of a obtaining a driving licence. You always need to start off by first learning how to drive. The better you can drive, the easier it is to pass the test. Equally, no amount of learning the Highway Code in itself will enable you to pass, albeit that you need to understand the rules. In the same way, the more efficient you are with the handling of your data – knowing where it is, making it secure, avoiding duplication and having transparent and simple processes will not only greatly assist with compliance, but will also result in a more efficient operation, with the associated business benefits.

Some years ago, I worked on the Millennium Bug programme – also known as Y2K. Many of you may not remember this – or merely wish to forget! At the time, this was a big programme of work for organisations. They needed to identify any data that may be subject to date problems as the clocks turned to 1st January 2000. It was very similar to GDPR as a compliance issue, in particular given its time base imperative. That is, how to identify and then make secure the relevant data.

The organisation that I was consulting at decided to use the opportunity to consolidate their processes and systems and reduce the diversity of applications. This provided a tangible and sustainable business benefit going forwards. So this model can be used again. That is, use the money invested to sustain some advantage

.

So what does an organisation need to do to comply with the GDPR? What can be done to turn what may be considered a purely compliance issue into a tangible business benefit? If we turn on its head the question of compliance we can pose the question; could our data handling in terms of processing and storage be improved such that we can be more efficient? In other words, can we adopt slick processes and efficient storage mechanisms to thereby provide essential management information as a by-product of compliance?

What Steps should be taken?

So what can be done to ensure compliance and accrue the business benefits in so doing? Well, there are a number of steps that can be taken right now. These are not linear and can be undertaken concurrently.

Step One – Do I process any personal data - What is the Lawful Basis?

First of all, you need to establish if you do in fact process any personal data. As stated, this is defined as any information relating to an identifiable person who can be directly or indirectly identified. So, if you do not capture any of this information then you will not be affected. If you look at this closer however, you would have to have no employees or customers or shareholders or any interaction with any category of Data Subject. Equally, you would not be acting in the role of either Controller or Processor.

There are 6 Lawful Bases for processing personal data.

1. Consent

This is where the individual - known the Data Subject has given clear permission (consent) for you to process their personal data. this must be for for a specific purpose.

2. Contract

The processing of personal data is necessary to discharge your duties for a contract you have with the individual, or where they have asked you to take specific steps before entering into a contract.

3. Legal Obligation

The processing is necessary for you to comply with the law - any legal obligations that you may have that are specific to your industry or applicable to all.

4. Vital interests

This is where the processing is necessary to protect someone's life.

5. Public task

The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law

6. Legitimate interests

This is the lawful basis that most small, commercial businesses will probably choose for processing their customer's personal data.

Step Two – Are we the Controller of Processor – or both?

The Controller is the organisation that determines the purposes and means of processing personal data and the Processor is responsible for processing personal data on behalf of the former. So the second step is to decide if you are acting as Controller or Processor. This is of particular concern if you are sending data outside of the EU for processing, see below. Outsourcing of the payroll to the accountants is one such example.

Step Three – Undertake an Audit

The Third step is to undertake an audit of all personal data held. This can be achieved by the completion of a Data Inventory that details both the processing and the storage of data. It is also known as Record of Processing Activity or ROPA.

Article 30 of the GDPR states;

The obligation to create records of processing activities is not only imposed on the controller and their representative, but also directly on the processor and their representatives as set forth in Art. 30(2) of the GDPR. For a change, companies or institutions with fewer than 250 employees are exempt from keeping a record, if the processing is not likely to pose a risk to the rights and freedoms of the data subject, if no special categories of data are processed or if the processing is done only occasionally, as is indicated in Art. 30(5) GDPR. In practice, this exemption is rarely applicable.

his produces a matrix of who does what to which data, why and how and at which frequency. This data may be held in either electronic or paper formats. Electronic data is categorised as either Structured or Unstructured. Structured Electronic data includes database systems.

It is not an obligation therefore to produce a ROPA if you are small business. In my experience however, I believe that it is prudent to do so. This is because it is a good exercise to undertake to ensure that you understand all of your processing activities and to ensure that you know where duplicating of processing exists and where security may be lax. it also shows that you are adopting a gold plated level to your compliance.

Personal data may be held in either electronic or paper formats. Electronic data is categorised as either Structured or Unstructured. Structured Electronic data includes database systems. These are the easiest to deal with as validation rules are applied at the data entry point and storage and access and security can easily be applied. The use of Data Mapping, a technique to understand and document the flows of data within and without the organisation is essential.

Managing Unstructured Electronic data is more difficult when you use spreadsheets for holding key data - by proliferating the spread of data and processing and making tracking, access and security more onerous. Even trickier are emails and especially embedded documents – where people use the email system to retain documents within that filing system. Paper can be a further challenge if there isn't a proper records system and it is more difficult to maintain security. The more complicated or wider the processing and the greater the use of unstructured electronic and paper records, the greater the challenge and hence risk from GDPR.

Step Four – Is any processing outside of the EU?

You will also need to ascertain whether any data is processed on your behalf outside of the EU – by a Processor, on your behalf. If so, you will need to look at the contracts and ensure that the processes and procedures are GDPR compliant

Step Five – Produce a Gap Analysis

From The Data Inventory and with a full understanding of what personal data is held, how it is processed and stored the fifth step is to produce Gap and Risk Analysis. This will establish what needs to be done and help with prioritisation by factoring in the risk.

Step Six – Cyber Security

Data protection legislation has at its core, the principle of Information Security. This was stipulated in the Data Protection Act of 1998 as Principle 7 - Personal data must be kept secure. The General Data Protection Regulation (GDPR) also includes this aspect of data security as Principle 6 – see above - Integrity and Confidentiality. Data must be “processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures”.

I would highly recommend obtaining the Cyber Essentials certification. This will tell your Stakeholders that you have a level of maturity, maintain this and help you win business. Having this certification will quickly move to being mandatory for companies wishing to engage with vendors and customers.

Cyber Security is all about understanding external threats, assessing vulnerabilities and risks and applying controls and monitoring to provide protection to your data. This is the most likely cause of a major data breach and the ICO fines heavily those organisations that have their data compromised.

Step Seven – Education, Training and Communications

The Seventh Step is about ensuring that your staff is educated about GDPR. The Regulation concentrates on the idea of putting data protection awareness at the centre of an organisation. There is plenty of material on the web, especially that published by the ICO and we also have lots of material that can be used.

Step Eight – Handling Requests from Data Subjects

The Eighth Step is to make sure that you are ready for all personal data processing activities post 25th May 2018. Especially for dealing with your customers and the general public, you need to have in place a process to handle Subject Access Requests or any other interaction with regard to personal data.

Step Nine – Anonymisation and Pseudonymisation of data

The Ninth Step is to see if you can anonymise or pseudonymise any of the personal data to reduce the risk of a data loss. Anonymisation is the most secure. This is involves storing data into a form which does not identify individuals. Pseudonymisation is the separation of data from direct identifiers so that linkage to an identity is not possible without additional information that is held separately. This greatly reduces the risk of data loss or exposure.

Step Ten – Implement the appropriate governance

The Tenth Step is to put in place the right governance to ensure that the work that you have undertaken to achieve compliance is maintained and that future proposed changes include Data Protection by Design and Data and Protection Impact Assessments to account for and asses the risk to personal data.

Step Eleven – Monitoring and Ongoing audits

Finally ensure that you undertake audits to provide evidence that you are maintaining vigilance, take into account the decisions that will be published by the Information Commissioners Office (ICO) on the subject and look at their Guidance Notice

Also, investigate some of the software that already exists and is being developed to help you with granular level GDPR data identification. All of this will provide evidence that you are putting the Data Subject's rights at the top of your priorities. This will greatly protect you in case of any breaches occurring.

In Conclusion

In conclusion, GDPR can be a wake-up call to sort out your processes, procedures and technology and thereby run a more successful organisation. Data is now more essential than ever, regardless of your activities or market sector. Not only will efficiencies accrue but being able to state with confidence that you are GDPR compliant will give you an edge over your competitors.

This is the ‘Carrot’. The ’Stick’ is the danger that a PPI type industry of claims will emerge. Article 79 (of the Regulation) provides the Data Subject with the right to an effective judicial remedy against a controller or processor, Article 82 with the Right to compensation and liability and Article 83 with regulatory fines.

The Author - Thomas Hayes

Thomas Hayes has more than 30 years practical experience in; business analysis, project management, Information Management & Governance, Data Protection as well as business up to Managing Director level, managing large business change and transformation.

He has provided consultancy services within many private and public sectors within. Europe, USA and China.

He has the following formal qualifications; • BA Honours in Politics & Contemporary History • Part-qualified Accountant ACMA Professional Part 2 • Association for Project Management qualified • Certificate in Information Governance for Health & Social Care • Fellow of the British Computer Society • BCS Chartered IT Practitioner • GDPR Foundation & Practitioner Certificate • IAPP Fellow, CIPP/E, CIPM • BCS CISMP • Certified Cyber Security Practitioner pending • Advanced Diplomas in Stress Management, NLP, Life Coaching, TEFL and Advanced TEFL• Published Author

.

Website; **www.hayesltd.com**

Email: **thayes@hayesltd.com**

Contact Telephone: **07834 039328**