Digital Marketing

Data Compliance Requirements

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

Hayes Associates Limited

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 Digital Marketing company needs to consider when processing personal data. It summarises the key facts that are salient to your business when considering data governance.

Digital marketing and the use of personal data to undertake your business forms a synthesis at the very core of your operation. Without data and its 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?

There are three main elements to consider. The first is the *General Data Protection Regulation (GDPR)*. The second is the *Privacy Electronic Communication Regulation (PECR)*.The third is the subject of how to provide controls to protect this data. This is ***Cyber Security***, and is a subset of the two primary legal frameworks. It also is of major importance in ensuring that your data - your lifeblood for your company, is available and accessible at all times. This is a major business objective - over aabove the compliance requirements.

The key to success in all of this is to strike a balance between that on the one hand, of applying the rules too restrictively to that of the other - having a lack of awareness. Not all communication to customers is regarded as being that of Direct Marketing - defined as - any type of sales promotion. Included in the definition however, are activities that are not primarily for financial gain. These include the activities of non commercial organisations - such as charities and political parties.

Data Protection applies to Direct Marketing when it is directed at particular individuals. That is, where personal data is processed in order to undertake the marketing. This therefore excludes information such as website banner advertising, non specific individual targeting and information as to the status of general services and products purchased by the customer.

General Data Protection Regulation (GDPR)

One set of rules that needs to be complied with are those enshrined in the General Data Protection Regulation (GDPR) that was enacted on May 25th 2018. This is just the latest piece 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 lassitude. For example; immigration data and age of children's consent. In actual fact, the GDPR wasn't a dramatic change. What generated all of the attention was the level of fines that could be applied – up to 4% of turnover.

Under GDPR, a company needs to have a lawful basis for the processing of personal data. There are six lawful bases allowable. These are; Consent, Contract, Legal Obligation, Vital Interests, Public task and Legitimate Interests. Consent is the most difficult as it may be withdrawn by the Data Subject and records of the Consent need to be maintained.

Marketing and Data Compliance

GDPR applies to **all** processing of personal data. This also includes Business to Business transactions. It provides Data Subjects – those individuals whose data is being processed by another entity, with a number of rights. These include; provision of Information about what is held, access to such, rectification of errors, withdrawal of consent to continue to process and objection. The key point to understand is that the data belongs to the Data Subject, not the company processing it.

Prior to 25th May 2018, many organisations had made the mistake of requesting consent, often when the individual didn't even know that any data was held about them and in most cases when requested to do so, didn't respond with an affirmative. This significantly reduced the available data in situations where only about 20% of individuals replied to the endless emails that they were bombarded with during the lead up to that GDPR deadline. Consent is only one of 6 Lawful bases for the processing of personal data and is the hardest to comply with. This is due to the ability of the Data Subject to withdraw such Consent at any time and the need to keep accurate records of the whole process.

The GDPR applies to all marketing whether Digital or not. Digital Marketing communications also has to comply with the Privacy Electronic Communications Regulation (PECR), also known as the E-Privacy Directive. This is covered immediately below. The minimum and initial steps required to comply with the GDPR are as follows;

1. Provide the Lawful Basis for processing of personal data - Legitimate Interest
2. Publish a Privacy Notice on your website
3. Implement an Information (Cyber) Security regime
4. Undertake a full audit of data processing activity

Legitimate Interests is a much safer option, albeit that this could be challenged by the Data Subject. You need to show that how you use people's data is proportionate, has a minimal privacy impact, and that the Data Subject would not be surprised or likely to object to what you are doing.

Privacy Electronic Communications Regulation (PECR)

For Direct Marketing using electronic media, there is an addition (EU) regulation. This is known as ***The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).*** It is also known as the E-Privacy Directive.

The rules under this regulation apply to texts, emails, marketing calls, emails, texts, faxes and cookies (and similar technologies). It only applies where there media used are *publicly available*. These require Consent from the Data Subject for Direct Marketing activity.

The GDPR was preceded by, and does not replace PECR, but it does change the underlying definition of Consent. The PECR rules that existed prior to, and continue post GDPR (after 25th May 2018) still apply, but now require the standards for Consent to meet those laid out under the GDPR. This means that if you do send out any electronic marketing or use cookies on your website or adopt similar methods then you must comply with both of the regulations.

PECR also requires that communications services are secure. This is also part of the GDPR as it was with all other Data Protection legislation and guidance that preceded it. There also needs to be adherence to customer privacy as regards; traffic and location data, itemised billing, line identification, and directory listings.

PECR also applies to cookies used on your website. This is why you see the consent questions on websites that you visit and the need for consent to be given before you proceed further. The PECR is due to be updated. It was scheduled for this to happen at the same time as GDPR but this deadline has been missed. It now seems likely that Brexit will supersede this EU legislation. For more information on Brexit and Data Protection please see my ebook on this subject.

Cookies are classified broadly as of two types - Essential and Non-Essential. Essential Cookies do not require Consent from the Customer or User. In essence, if the functionality of the Cookie is what the User would reasonably expect and is not intrusive, then this would be classified as Essential. For example, if used solely to ease the use of the software by the User - remembering information such as baskets ready for check-out on purchases. Non-Essential Cookies require Consent from the User.

The PECR does not apply to telephone marketing from person to person. There is also some limited exemption for businesses to send marketing to *existing customers* for *similar products*. That is Consent is not required in these circumstances.

Cyber Security

One of the six (or seven - if you include Accountability) GDPR principles that has been at the forefront of all data protection, is that of security. It was also one of the Eight Principles in the Data Protection Act of 1998. This means that you must process personal data securely by using 'appropriate technical and organisational measures'. This leads on to the third element in the equation **- *Cyber Security.***

The term *Cyber Security* is a relatively new. The word *cyber* is an abbreviation of the Greek word *cybernetic.* This means *skilled in steering or governing. Security* means *freedom from, or resilience against, potential harm*. Hence the term *Cyber Security* denotes the means by which to prevent harm. In the modern technological context, this means the protection against harm to the systems that are used for the processing of information. For further information, please refer to my ebook *Cyber Security for Small Business.*

First and foremost, Cyber Security is a form of protection against threats to electronic equipment used by organisations and individuals. It is a defence against malicious attacks on hardware such as; computers, servers, mobile devices, electronic systems, and networks. It also includes protection for software and data processed and stored on associated hardware.

Marketing and Data Compliance

Cyber Security deploys technologies, processes and controls to protect against malicious (external) attacks as well as education, awareness, and adequate policies and procedures. The aim of cyber security is to reduce the risk of any cyber-attacks. Accreditation in terms of International standards such as ***ISO 27001*** for Risk Management and ***Cyber Essentials*** - an accreditation. scheme within the UK, will not only provide evidence of compliance but will prove to be a great advantage in winning business. Indeed, in the near future this will be stipulated requirement in contracts.

ISO 27001 is a specification for an ISMS that is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

Cyber Essentials is implemented to guard against the most common cyber threats and demonstrate your commitment to cyber security through a formal independent assessment and accreditation.

In order to be confident that you are complying with the requirements of GDPR, PECR and Cyber Security, there are a number of steps that can be taken. The first is to adopt the understanding that compliance has two halves; the rules and the operations against which those are set against.

Understanding the rules can be outsourced to an expert or training acquired. In terms of operational activity, having an effective and efficient information management regime is crucial. It also provides business benefits in terms of reduced costs and better processing, storage and dissemination mechanisms.

Checklist

There is excellent and detailed guidance on the ICO website. There is also a good summary Checklist that can be found here - below. It can be used to check compliance when considering Direct Marketing by electronic means.

ICO Checklist

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**