GDPR

“DATA PROTECTION BY DESIGN AND BY DEFAULT”

The new General Data Protection Regulations could make your customer data unusable for ALL sales & marketing activities. Act NOW to stop that happening.

AVOIDING DATA ARMAGEDDON!

GDPR

"DATA PROTECTION BY DESIGN AND BY DEFAULT"

The new General Data Protection Regulations could make your customer data unusable for ALL sales & marketing activities. Act NOW to stop that happening.

This document was written and designed by Michael Payton of Payton Marketing Ltd.

Michael Payton is a marketing consultant and GDPR subject-expert.

Michael Payton

Marketing Consultant and Practitioner

07764 959 030

michael@paytonmarketing.com

LinkedIn: Michael Payton MBA MCIM

www.paytonmarketing.com

NOVEMBER 2017

Why you should read this document

The new **General Data Protection Regulations** (GDPR) come into force on 25 May 2018.

If you don't take action RIGHT NOW, the use of all your customer data could be illegal from that day onwards.

This document does 3 things:

1. It **tells you quickly** whether your company could be affected.
2. It **explains the regulations** and the massively increased sanctions that can be imposed.
3. **It outlines the steps you need to take NOW to avoid losing your customer and prospect data.**

Even business-to-business (**B2B**) organisations have no easy way around the new rules. There's a section dedicated to B2B that tells you what you need to know.

Think **Brexit** will make a difference? Think again. GDPR comes into force a full year before we're due to leave the EU. And afterwards . . . we'll still have to conform!

This document provides your starting point. It gives you a framework for a '**GDPR-Compliance**' project and links to lots of further information and official documents.

And if you need further help and advice you can contact me, **Michael Payton,** using the information on page 2.

The ways you're allowed to use personal data are changing. Rules are being tightened and sanctions are being increased. You may not be able to keep all your data once the new regulations are in force, even if you start complying right now.

But the danger lies in doing nothing. If that's your strategy, you could end up with no legal way of contacting any of your existing customers and prospects ever again!

michael@paytonmarketing.com | 07764 959 030 |

Contents

Why you should read this document 3

Do the regulations apply to my business? 5

Background to the new regulations 6

The GDPR in brief 7-9

Info Block: What is personal data 7

Info Block: Subject Access Requests 8

Info Block: Emails and unstructured data 9

Accountability and Governance 10

Info Block: The Data Protection Officer (DPO) 10

Setting up a GDPR project 11

Your Information Audit 12

B2B – what you need to know 13

Gaining Consent 14

Info Block: Employees as well as customers? 14

Data breaches and breach notifications 15

Sanctions and fines 16

Brexit 17

Info Block: "Legitimate Interest"? 17

Help with your project 18

Further information, resources and links 18

michael@paytonmarketing.com | 07764 959 030 |

Do the regulations apply to my business?

In the official language, the regulations apply to 'controllers' and 'processors' of data. **In reality, that means all businesses** and other organisations that have customers and/or staff.

'Data processing' covers things like collecting, recording, storage, alteration, retrieval, use, disclosure and erasure of personal information.

The 'data controller' is the organisation (or person) that determines what happens to the data. The 'data processor' is the organisation (or person) that actually handles the data.

So **most organisations will be both controllers and processors**, while some will process data on behalf of others (IT companies for instance).

For the **B2B** organisation, look at the definition of 'personal data' on page 7. If you handle personal data, and you are either a controller or processor of that data, then your business **is** covered by the regulations.

michael@paytonmarketing.com | 07764 959 030 |

Background to the new regulations

The official line is that any company fully complying with the Data Protection Act 1998 will not find the new regulations too onerous.

But as you'll see as you read further, that simply isn't true. The new rules outlaw previously accepted procedures, add considerable levels of bureaucracy and administration, and necessitate the setting up of a major compliance project even for relatively small organisations.

That's not to say the new rules are unnecessary. In fact they're well overdue! But the fact remains that compliance is likely to be an expensive and time-consuming race against time.

It's also safe to say that not every company will survive the transition, especially those that don't plan in advance.

Data Protection is a dry, dull subject (even for those of us employed to know about these things), but when your whole business is being put at risk you definitely need to understand what's changing and what you need to do.

☑ *Don't want to hear more from us or our specially selected partners?*

Just untick this box and we'll ensure you hear no more about our great product and service offerings by phone, email or post.

Wrong in so many ways! Opt-outs like this will be explicitly forbidden. As will language, designs and fonts that make it difficult to read or understand.

michael@paytonmarketing.com | 07764 959 030 |

The GDPR in brief*

* For more detail on all of this, follow the Further Information links on the back page

The legislation comes into force on 25th May 2018.

It applies to any organisation or individual who uses the personal data of others.

Your main responsibilities for the handling of data are:

- Data must be processed **lawfully, fairly and transparently**.
- It must be collected and used for **specific, explicit and legitimate purposes**.
- It must be **limited to what is necessary** to fulfil the stated purpose.
- It must be **accurate** and, where applicable, kept **up to date**.
- Data must be kept in a form which permits the identification of the individual for **no longer than necessary**.
- It must be used in ways that ensure the **security** of the data.
- You must be able to **demonstrate** compliance with these principles.

What is 'Personal Data'?

'Personal data' is defined as any piece of information that relates to, or can be traced back to, an identifiable person.

So as well as covering the obvious - name, address etc - it also covers things like a reference number, their IP address, sales records and even the contents of emails.

It's the same for B2B companies. If you can link the data to an individual – such as the sales manager for instance – then it's personal data.

If a piece of data can be linked - directly or indirectly - to an individual, it's personal data.

michael@paytonmarketing.com | 07764 959 030 |

The GDPR in brief*

* For more detail on all of this, follow the Further Information links on the back page

The individual who's data you hold has the following rights:

The right to be informed: You must tell people up-front what you will use the data for.

The right of access: On request, you must supply all pieces of data you hold which relate to the individual, free of charge, within 30 days.

The right to rectification: You must rectify incorrect or incomplete data, and you must inform any third parties to whom you have disclosed this data.

The right to erasure: Also known as the 'right to be forgotten', the individual has the right to have their personal data erased.

The right to restrict processing: The individual has the right to require you to stop using the data in any way, whilst not deleting it from your records.

The right to data portability: This gives the person the right to move their data from your records to a different supplier. This is restricted to data they have supplied to you, so does not include sales records etc.

Subject Access Requests

Individuals have a right to know what data you have about them and what you do with it. When they ask for this information it is called a 'Subject Access Request'.

You must provide this information free of charge (currently you could apply a £10 charge).*

You must send every piece of information you hold about the individual, either in paper format or in a 'commonly used' electronic format (MS Office programs for instance).

The time limit for you to respond has decreased from 40 days to 30 days.

** There are circumstances where a 'reasonable fee' can be charged. See the 'Overview of the GDPR' document on the Further Information page*

michael@paytonmarketing.com | 07764 959 030 |

The GDPR in brief*

* For more detail on all of this, see the Further Information links on the back page

The individual who's data you hold has the following rights (continued):

The right to object: Individuals have the right to object to the use of personal data for any purpose (such as for direct marketing). If the objection is valid, you must stop using it for that purpose.

Rights relating to automated decisions and profiling: A person has the right not to be subject to a decision that is based solely on automated processes. You must then provide human intervention taking into account their individual circumstances and their point of view, and you must provide an explanation of your final decision.

Emails and 'unstructured' data

The content of emails can be construed as personal data.

- *If you receive an email from an individual and if the contents can be traced back to that individual, the whole content falls within the regulations.*
- *If you send an internal email, and within the email is information relating to individuals that can be traced back to those individuals, then this also counts.*

Managing the content of emails will be tricky to say the least. Data must be indexed in a way that allows you to respond to Subject Access Requests. You should consider policies that limit what is said and develop retention policies for the storage and deletion of old emails.

Consider storing all emails on a shared server or shared drive, and not on individual computers.

Data held on other devices can also be deemed 'personal information'. On mobile phones, phone numbers, contact information, even the contents of text message will count if you can trace the contents back to an individual.

michael@paytonmarketing.com | 07764 959 030 |

Accountability and Governance

You must be able to demonstrate your compliance with the principles and rights of the legislation.

In brief, this means:

Providing sufficient data protection policies such as staff training, internal audits, HR policies etc.

Maintaining relevant documentation on all processing activites.

Implementing measures that adhere to the policy of 'DATA PROTECTION BY DESIGN AND DEFAULT', including:

- Data minimisation
- Psuedonymisation
- Transparency

Using data protection 'impact assessments'.

You must appoint a Data Protection Officer where required, or a named individual with responsibility for Data Protection practices.

The Data Protection Officer (DPO)

You must appoint a DPO if you:

- Carry out large-scale monitoring of data (eg of online behaviour).
- Process data relating to criminal convictions and offences
- If you are a public body.

If you do not appoint a DPO, you must ensure your organisation has the formal capacity to conform to the GDPR's requirements.

The DPO (or responsible person) can be an internal appointment or an external contractor. They must have sufficient knowledge and experience of data protection law, and there must not be a conflict of interest with their day-to-day job (so an IT manager or sales & marketing manager is not appropriate).

The DPO must report to the highest level of authority in the organisation, at least indirectly.

They must have adequate resources to do the job – time, access and budget.

michael@paytonmarketing.com | 07764 959 030 |

Setting up a GDPR Project

You've got a lot to do to ensure you can still use your customer data for sales and marketing purposes after May 25th.

A **cross-departmental project** is a good idea. In this way you've got a good chance of catching everything and giving yourself the best possible chance of success.

Use the project to:

- Audit what you've currently got and what you do with it.
- Identify breaches, risks and gaps
- Develop plans for putting things right
- Monitor your progress

But don't let your project stop you acting NOW if you know you've got things to fix.

If you can't prove your customers positively opted-in to receive your information, then don't wait for a project to tell you in a couple of months time – sort it out now!

Mail them now (where you have current permission to do so) and start asking them to opt-in to communications. The sooner you start, the more chances you've got.

Yes, you will lose some. but that's better than losing them all in a few months time!

You may need a subject-expert to act as project sponsor – someone who can independently report to the Board on your progress, and who can direct the project towards the most important outcomes.

Payton Marketing can provide you with professional advice, and may even be able to act as your project sponsor. Call or email now for more details.

michael@paytonmarketing.com | 07764 959 030 |

Your 'Information Audit'

This is the first stage of your GDPR project – until you know exactly what information you hold and what every department does with it, you can't hope to reach compliance.

Your audit will reflect your own company structure and procedures, but here are three tools you should consider using:

1. Data Maps

Create detailed flow diagrams (with supporting documentation) outlining where personal data comes from, how it is input, who uses it (and how) and when it is deleted.

2. Asset Register

Using the Data Maps, compile a register of all the data you hold. This should cover the name of the asset (eg, your CRM database), its location, who in your organisation 'owns' the asset, a complete list of all the information fields, who has access (internal and external), and details of your retention policies.

3. Risk Assessment

For each asset outline the risks, including data breaches, data loss, usage loss and so on. Use this to help you plug the risks and make your data more secure.

michael@paytonmarketing.com | 07764 959 030 |

B2B

Under the current regulations (the Data Protection Act 1998 and the Privacy & Electronic Communications Regulation (PECR) business-to-business organisations were *largely* left alone and could *pretty much* contact any business-contact they liked without *very much* fear of official sanction. I exaggerate. But only a little.

All this changes on 25th May 2018.

Personal data is personal data - full stop. It doesn't matter anymore that you're only contacting them on behalf of the company they work for. If you can identify an individual from the data record, then that whole record becomes personal data.

So if you've got a business record with a named individual linked to it, that is personal data and is subject to the regulations.

What makes this scary and problematic is that it also (by definition) makes the record open to a Subject Access Request, whereby you would have to disclose every bit of data that's linked to their record, whether or not the information is commercially sensitive!

We have asked for clarification on this point from the ICO (Information Commissioner's Office) and will update every contact (where you've given permission of course) when we hear back.

There are circumstances where the rules won't apply. Data that is not linked to an identifiable individual is not 'personal data'. So if your record simply holds the job title 'Purchasing Manager' and the contact number is a land-line rather than a personal mobile, then that record will probably be clear of the regulations.

But de-personalising your data in this way is a drastic step and flies against every objective of your CRM database.

So overall, much of your customer and prospect data is likely to fall within the regulations and you simply *have* to conform.

For clarification of the Subject Access Request issue, make sure we have permission to contact you and we will let you know what we hear.

michael@paytonmarketing.com | 07764 959 030 |

Gaining Consent

The general principle here is to give genuine choice and control to the individual. Consent is defined as the 'freely given, specific, informed and unambiguous' agreement to the use of personal data.

Things to note about the concept of consent are:

- It requires a positive opt-in
- Consent requests cannot be hidden inside other terms and conditions – they must be separate.
- Consent must be 'specific and granular'.
- You must name any third parties who will also rely on this consent.
- You must keep the evidence.
- You should not make consent a pre-condition of service.

Employees as well as Customers ?

Yes, personal information is the same whether it covers a customer or a member of staff. So you've got to treat it with the same care.

In reality, you'll need different processes and probably different people involved in the management of your HR data, but the principles are the same:

- Only collect and store the data you need, for as long as you need it.
- Don't use or disclose it without permission
- Don't allow it to be compromised
- Report any breaches immediately

There is a 40-page document on the ICO website about gaining consent. To download it, go the Further Information page at the back of this paper.

☐ We can send you further information from time to time by email. Please tick to confirm you would like to receive these emails.
We will never share your details with anyone else.

Clear, understandable and with a positive opt-in. The minimum standard for consent.

michael@paytonmarketing.com | 07764 959 030 |

Data breaches and breach notifications

Under the GDPR, you have a duty to inform the Information Commissioner's Office (ICO), and often the individuals concerned, of any significant data breaches.

A personal data breach is defined in the regulations as:

> ***"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".***

You must inform the ICO of a breach where the rights and freedoms of individuals are likely to be affected, including:

- financial loss
- loss of confidentiality
- damage to reputation
- discrimination
- any other significant economic or social disadvantage.

Where the risks to rights and freedoms are high, you must also notify the individuals concerned.

You must notify the ICO within 72 hours of becoming aware of the breach, and the individuals concerned 'without undue delay'.

Failure to notify the authorities or individuals of a breach can result in a fine of up to €10m or 2% of global turnover.

michael@paytonmarketing.com | 07764 959 030 |

Sanctions and Fines

The implications of non-conformance are far greater than under the current Data Protection Act. Maximum fines of €20m or 4% of gross global turnover can be imposed.

As a regulation not a law, punishments will be in the form of fines not prison.

The most likely series of sanctions against companies that breach the regulations will be:

- **Warning**
- **Official review of procedures**
- **Fine**

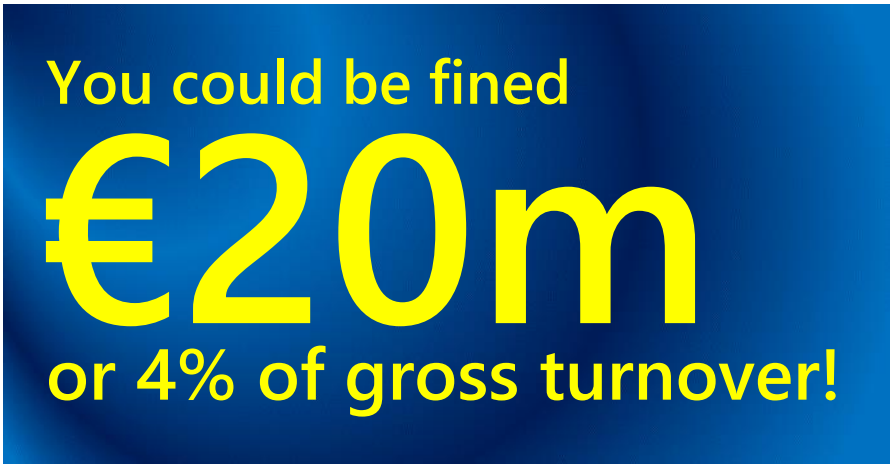
Under the current Data Protection Act (1998) the maximum fine is £0.5m.

The new regulations increase this to **€20m or 4%** of global turnover.

For the failure to notify the authorities or individuals of a data breach, the maximum fine is €10m or 2% of global turnover.

The Information Commissioner's Office (ICO) will have the power to:

- **request information**
- **enter premises**
- **inspect records and systems**
- **carry out audits**
- **dictate improvements.**



michael@paytonmarketing.com | 07764 959 030 |

Brexit

And finally a word on the elephant in the room – **Brexit**. Does everything change as soon as we leave the EU?

We don't know exactly when Brexit will happen, or how quickly it will be implemented when it does happen, or indeed what exactly will happen to all our laws once we're independent.

So here's what we do know:

- The GDPR will be implemented across the EU on 25th May 2018 – **a full year before we're due to leave.**
- After we've left, the government currently says the regulations will stand.
- If we want to do business in Europe, our Data Protection laws need to be at least as tight as the EUs. So the idea of going it alone doesn't seem to make sense.

The only sensible conclusion, currently at least, is that the GDPR will remain in force after Brexit.

"Legitimate Interest?"

At the time of writing there is a lot of uncertainty over other potential justifications for contacting customers and prospects (other than explicit consent).

The main area of doubt is over 'legitimate interest' and what this might mean for businesses. It seems possible that future guidance from the ICO will give companies more flexibility and/or freedom to continue to contact individuals even without explicit consent.

At present, however, we just don't know what the guidance will say, or even whether it will appear at all, and we will await clarification.

michael@paytonmarketing.com | 07764 959 030 |

Need help with your project?

You need to set up a project to ensure you hit the deadlines, conform to the new regulations and can continue to use your data for all your normal business process and marketing activities.

Your GDPR project needs to be led by a subject-expert. Someone who can independently report to the Board on progress, and who can direct the project towards the most important outcomes.

Payton Marketing can provide you with professional advice, and may be able to act as your project sponsor.

Call or email now:

Michael Payton MBA MCIM on 07764 959 303

michael@paytonmarketing.com

Further Information

The Regulations themselves

You can find an excellent, indexed copy of the legislation here: https://gdpr-info.eu/

The Information Commissioner's Office (ICO)

The ICO website is here: https://ico.org.uk/for-organisations/data-protection-reform/

12-step preparation document: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Overview of the GDPR: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

GDPR Consent Guidance: https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

Government Papers

Department for Digital & Culture Statement of Intent: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635900/2017-08-07_DP_Bill_-_Statement_of_Intent.pdf

House of Commons Library, Briefing Paper: http://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7838

