GDPR for marketers: Accountability

In partnership with

Contents

Welcome to GDPR guidance for marketers

May 25, 2018 will see the new regulatory framework take effect – and it offers all of us the greatest opportunity for business transformation in a generation.

The General Data Protection Regulation (GDPR) mirrors the DMA's long-held view about the need to place people at the heart of everything we do – and echoes our commitment to a code that enshrines five key principles which marketers should follow:

- Put your customer first
- Respect privacy and meet your customers' expectations
- Be honest, be fair, be transparent
- Exercise diligence with data
- Take responsibility, be accountable.

The DMA has actively influenced the evolution of the GDPR text since first drafts were circulated by the EU Commission in 2011, supported by our expert partners at the Advertising Association in London and FEDMA in Europe. We have worked closely with our partners in government and across the wider marketing community throughout the draft process.

Our advocacy has established vital building blocks within the GDPR that will safeguard the interests of our members and bolster the wider marketing community. Of particular importance to marketers is the clear statement in Recital 47 that the processing of personal data for direct marketing may be regarded as being carried out for legitimate interests.

To support business transition to this new data landscape, we have crafted a guidance series that examines the GDPR through a marketer's lens.

This guide, GDPR for Marketers: Accountability, is one of a series providing marketers with a framework for innovation and growth. Other guides take an in-depth look at the essentials of GDPR, Legitimate Interests, Consent and Profiling.

While ICO and Article 29 working party guidance apply across all business sectors and functions, this DMA series aims to be the definitive guidance for applying GDPR to marketing and communications. That is why we have collaborated with our DMA members, the members of ISBA, and the Data Protection Network to produce a consensus view.

Our work has been reviewed and contributed to by the ICO and we are grateful for their support.

The DMA believe that organisations must use GDPR as a catalyst towards creating people-centric business models. From the C-suite down we must all create ethical approaches that balance innovation and privacy as we embark on a journey into the fourth industrial revolution powered by data and technology.

Businesses that make data protection a core brand value in the years ahead will blossom.

Chris Combemale
CEO, DMA Group

Foreword by the Information Commissioner

This is a pivotal time for data protection and privacy.

We have a digital infrastructure that was unimaginable 20 years ago and data protection laws are converging across the globe. Consumer trust is ever more central to both business and the public sector, and a rapidly expanding digital economy is asking more questions of us all.

For me, the end game in the data protection field is always about increasing public trust and confidence in how their personal data is used.

Data protection reforms, including the GDPR, build on previous legislation, and provide more protections for consumers, and more privacy considerations for organisations. But this is a step-change. It's evolution, not revolution.

It's vital that organisations are prepared to comply but they can also prosper in the new regulatory landscape.

If your organisation can demonstrate that good data protection is a cornerstone of your business policy and practices, you'll see a real business benefit.

An upfront investment in privacy fundamentals offers a payoff down the line, not just in better legal compliance, but a competitive edge. I believe there is a real opportunity for organisations to present themselves on the basis of how they understand and respect the privacy of individuals.

This helpful guidance has been drafted by the DMA with its members, members of ISBA and the Data Protection Network with input from the ICO. It will help marketers navigate through the GDPR and complements our own GDPR guidance and additional online checklists and resources.

I hope this guidance helps you be transparent, accountable and ensure people have appropriate control over their personal data.

Elizabeth Denham
Information Commissioner

The DMA and the GDPR

How we create GDPR guidance

The GDPR Editorial Board leads the content direction of the DMA's GDPR outputs. We inform the work with expert advice and guidance from our Responsible Marketing Committee and the specially-appointed GDPR Taskforce.

To generate the right content for the right channels, the GDPR Editorial Board, Responsible Marketing Committee and the GDPR Taskforce work in collaboration with our Councils. This focuses our work onto the immediate needs of the marketers we serve.

Throughout our approach to preparing the industry for the GDPR, we work with the ICO and partner with:

Introduction

"A body of men holding themselves accountable to nobody ought not to be trusted by anybody."
By Thomas Paine from The Rights of Man, 1791

Paine was referring to the abuse of common French people by the aristocracy. It was a stout defence of the French Revolution, then well under way.

Fast forward to the present day and we sit on the cusp of another revolution: a total overhaul of how we work with information, the General Data Protection Regulation (GDPR).

At the heart of the GDPR is the power of accountability, a key driver to ensuring companies can truly demonstrate compliance with the new legislation.

And the regulation is not just about individual accountability, or the accountability of a group of individuals, but rather accountability across whole organisations.

UK organisations should seize upon GDPR as the catalyst to transform their operations to become customer centric.

They should use the principle of accountability as the foundation for an authentic and transparent relationship with their customers.

This instalment of the DMA's GDPR guidance covers:

- The concepts behind the principle of accountability
- What the principle of accountability will mean to your organisation
- The use of Data Protection Impact Assessments (DPIAs) to help demonstrate compliance
- The role of the Data Protection Officer (DPO) to manage, monitor and advise on GDPR compliance
- The importance of keeping records of processing activities

The ICO does emphasise the positive side of making these changes:

"Accountability encourages an upfront investment in privacy fundamentals, but it offers a payoff down the line, not just in better legal compliance, but a competitive edge. We believe there is a real opportunity for organisations to present themselves on the basis of how they respect the privacy of individuals and over time this can play more of a role in consumer choice."

What does accountability mean for marketers?

To put this topic into context, Information Commissioner Elizabeth Denham - who leads the ICO, which will regulate the GDPR in the UK - said to the Institute of Chartered Accountants in England and Wales on January 17th, 2017:

> ***Accountability is at the centre of all this: of getting it right today, getting it right in May 2018, and getting it right beyond that."***

The GDPR echoes the DMA's own longstanding code, which places the customer at the heart of all we do: the customer is the foundational principle for accountability and good marketing.

We believe there are three key accountability considerations for marketers:

- Accountability as a core principle

The GDPR has principles which apply to data processing. Data controllers are responsible for, and must be able to demonstrate, compliance with these.

Companies need to demonstrate compliance and be able to show why they need the data, what they are going to use it for, how they are going to keep it secure and the legal basis they are using to process the data, among other things.

- Accountability at the heart of operations

The company is responsible for what it does with its customers' data and has to consider the customers' right to privacy when developing new products, services or marketing campaigns.

The notion of data protection by design and tools such as Data Protection Impact Assessments should become standard business processes.

- Accountability goes right to the top

Accountability should be driven at board level – it's not just an issue for the lawyers. Ensuring an organisation builds a culture of accountability, transparency and trust is the responsibility of the CEO working closely with the data protection officer (DPO).

A DPO will be required by law for any organisation that works with significant amounts of personal data, among other requirements. The DPO must also be independent and report to the highest level within the organisation.

Accountability will be a business transformation driver
Accountability under the GDPR puts the onus onto organisations to change.

What will this mean in practice?

Many of the processes and templates that should be used to support a culture of accountability are essentially balancing tests to strike an equilibrium between competing rights. Documenting the results of balancing tests is how an organisation would evidence its compliance with GDPR.

For instance, Recital 47 states clearly that direct marketing is a legitimate interest provided it meets the reasonable expectations of customers, and that their expectations have been established through clear and honest data notices and privacy policies. This applies except where other legislation does; for example, automated calls, email and SMS marketing to consumers requires consent under the Privacy and Electronic Communications Regulations (PECR).

Consider that marketers will need to create comprehensive - but proportionate - governance measures; they must adapt to the legal requirements for the provision of Data Protection Impact Assessments and data protection by design; ramp up the documentation of activity and adhere to new codes of practice.

Fundamentally, accountability requires marketers to interrogate their processes by making sure data is collected lawfully, fairly and transparently in the first place, securely stored, and legally and securely processed or moved. Ultimately, it is about being able to produce evidence that you have complied with GDPR.

Furthermore:

- Those businesses that can demonstrate accountability will build trust with customers
- Those that can't will not be subject to data mishaps, which will damage trust in their brand, and also harsher fines
- In an enforcement decision, the ICO will take into consideration an organisation's attempt to stick to the principle of accountability, which could be seen as a mitigating factor.

It's not enough to comply with the regulation; you must be able to demonstrate compliance.

What is the accountability principle?

UK Information Commissioner Elizabeth Denham said in January 2017:

> ***"...arguably the biggest change [as a result of the GDPR is around accountability. The new legislation creates an onus on companies to understand the risks that they create for others, and to mitigate those risks.***
>
> ***"It's about moving away from seeing the law as a box-ticking exercise, and instead to work on a framework that can be used to build a culture of privacy that pervades an entire organisation."***

This is a powerful statement to make and heralds one of the largest programmes of change for British business for many decades.

Explaining the accountability principle

The principle of accountability, which underpins the GDPR, is referenced twice in the text: in Article 5(2) and in Recital 85.

The principle requires your organisation to be able to provide evidence that it complies with all the principles of GDPR. We recommend explicitly stating that this is your responsibility as a business.

The process of accountability is about having in place all of the policies and documentation necessary to demonstrate that what you are doing with consumer data is fair and compliant, and considers the right of consumers and the impact any data processing may have on them. If asked by a consumer about your data processing, you can easily refer to your agreed policies to explain.

Some specific obligations are imposed on your business to further the principle of accountability, including the need to give data subjects information about how their personal data will be processed. Articles 13 and 14 provide a breakdown of the information that needs to be provided to data subjects.

The biggest change for some organisations is the fundamental shift in power created by the GDPR.

Previously, businesses saw themselves as the owners of data, but the new regulations switch the power into the hands
of consumers. They have been given back control of their data, with new and stronger rights.

In the past, many organisations perceived that they "owned" people's data. Under GDPR, they are now required to ensure they only use it for as long as the consumer permits them.

The principle of accountability forces all companies to view what they do through the eyes of the customer. It makes them take a step back and look at everything they do with data and be able to produce evidence of why a decision was made.

They should have answers to questions like:

- Why are we collecting this?
- What legal grounds do we have to do this?
- What impact will it have?
- What are the risks to consumer privacy?
- How will the personal data be kept safe and secure?

By asking these questions, they will evolve their organisations to develop a genuine relationship with consumers, based on trust.

By taking a proactive approach to accountability, organisations can expect to:

- Make data processing more secure
- Have the ability to demonstrate that as much as possible has been done to make systems and procedures safe; and showing compliance with all the principles of GDPR
- Work transparently. The organisation should report any breach to the ICO within 72 hours, unless that breach is unlikely to result in a risk to the rights and freedoms of individuals.

What it means in practice

For organisations that deal with data, the GDPR is a major evolution of the current law, the 1998 Data Protection Act (DP98). For many, the new regulations will force a complete change of culture throughout teams and departments, if not the whole organisation.

As a minimum, the GDPR will force your business to reconsider the policies and processes it uses to manage and process customer and staff data.

Your business will need to examine the technical and organisational measures in place to ensure they conform to the standards laid down by GDPR. This step is essential for spotting and solving problems. Once these have been addressed, the organisation will be better able to demonstrate that it complies with the new regulation.

You must review what personal data you process - and how you process it - and reach a conclusion about whether your operation is compliant. Where you identify areas for improvement, you must make changes to ensure you have appropriate procedures, processes and technical and organisational methods in place, documenting these - including the work you have done to fill the gaps – as evidence that will show you are accountable under the GDPR.

The ICO has a useful toolkit to help with accountability in practice: https://ico.org.uk/for-organisations/business/

There are commercial benefits to businesses that can show they comply with the principle of accountability. Firstly, customers will have more confidence in a brand or organisation if they know it is compliant, safe in the knowledge data is being processed fairly and securely.

How do I ensure accountability?

Carrying out a data audit is a useful first step towards accountability. Use these three questions to create the core of your data audit approach:

Conclusion

Once you've formed a comprehensive picture of what personal data you store, you can begin to tackle the many other compliance challenges presented by the GDPR.

Auditing personal data is a first step.

And ahead of 25 May 2018 you will need to understand your legal basis for processing personal data you hold: for example whether or not you may need to delete any of that personal data.

About the DMA

The DMA provides guidance and support to help its members put their customers at the heart of their one-to-one communications to give them the rich benefits of a much more relevant, welcomed and effective relationship with each individual customer.

The DMA aspires to facilitate its members' marketing evolution with the opportunities, advice, support, networks and tools to be able to reach the sensitivity and sophistication of marketing to build their future prosperity – along with the success of the industry as a whole.

www.dma.org.uk

Privacy is a key ingredient of accountability. It should be baked into every process from the beginning.

Each organisation must make its own assessment, and take privacy into account when developing products and services.

Incorporate data protection by design principles, and ensure that training around data privacy goes beyond employees in the legal and compliance teams. It is everyone's responsibility.

Accountability must be top down, from the boardroom throughout the entire organisation, so that a cultural drive towards compliance can be demonstrated.

Data protection by design and data protection by default

These two elements, along with documentation, are the essence of the accountability principle. They entail making privacy a core brand value and building privacy features into all marketing activities.

Data protection by design: This is the notion that privacy should be considered by marketers at the beginning of the creative process. Privacy should not be an afterthought for the legal team to consider. It should be front and centre in the minds of marketers, and this means contemplating what privacy risks exist within a marketing campaign – as well as what could be done to mitigate those risks.

Data protection by default: This concept differs slightly as it relates directly to new software and products, so it's especially relevant for digital marketers. For example, an app on a smartphone facilitates the use of push notifications for marketing. Under data protection by default, the user should have to alter privacy settings to allow marketing via the app. For instance, many apps default to sending marketing via push notifications to the user.

Senior management should understand the importance of these principles and ensure their marketing staff know their importance, too.

This will require educating marketers about their responsibilities under the GDPR, also helping them to understand how in reality they can make privacy a core brand value.

There are various measures that can help to mitigate risks to individual privacy. Marketers should be aware of them, implement them where appropriate and ensure any steps towards demonstrating compliance are recorded, and are totally visible. Data Protection Impact Assessments (DPIAs) are tools designed to help organisations assess the privacy impact on individuals where the processing is likely to result in a high risk to their rights and freedoms. The assessment results can then be used to identify ways to mitigate the risks or take another approach to avoid them.

Data minimisation: This is the idea that marketing teams should only collect personal data that is required to meet their objectives. This has always been a key requirement of data protection law, but the GDPR emphasises it. For example, a direct mail campaign aimed at an affluent postcode area may only need names and addresses to succeed. Therefore, only names and addresses should be collected for marketing campaigns, rather than requests for emails and other types of personal data being made.

Data retention periods: This is where an organisation promises to only hold a piece of personal data for a limited period. It is also a key requirement of current data protection law. For example, when the marketing campaign is complete, then the personal data is deleted.

Encryption and hashing: Use these techniques to encrypt the personal data to prevent data subjects being identified in the event of a breach.

Transparency: Examine your privacy and information notices to ensure that they're written in clear and plain language suitable for your target audience. Using copywriters to craft your privacy notices is highly recommended, though not a requirement. See Articles 13 and 14 of the GDPR for the full list of information you must include in a privacy notice.

Preference centre: This is about giving people as much control as possible over the personal data you hold about them. For example, an organisation could allow people to access personal data held about them and update it on their website. DMA research shows that consumers want more control over their personal data.

All these measures help to lower privacy risks for individuals and are a crucial part of implementing privacy by design and privacy by default within your organisation.

A review of your existing data protection policies and procedures is a good starting point.

Once you understand the extent to which you are compliant, gaps can be identified, and you can then systematically prioritise them to make sure you comply in time for GDPR.

Case study – GForces approach to GDPR

GForces' clients can rely on the company to only use, store or process data vital to its business operations and to its clients'.

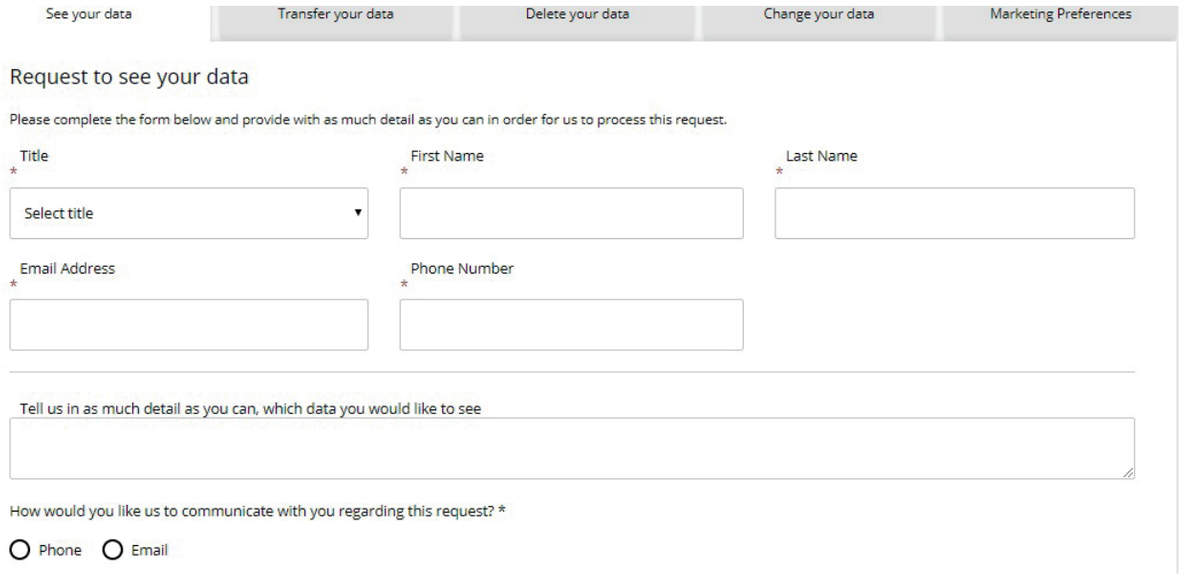
The software the company operates doesn't use automated decision making or profiling, and it continually improves security measures in line with certification.

The existing Data Protection Act afforded data subjects a number of rights – but many businesses did not provide an easy medium for those rights to be exercised.

GDPR provides data subjects with additional rights, so GForces created an easily accessible platform to accommodate these requirements.

In response to queries raised by clients and how they might be able to deal with potential requests, GForces built a data preferences centre - shown below - as a one-stop shop to address these concerns.

The centre is where a data subject exercises their rights under the GDPR to update their marketing preferences, see the data held on them and make specific requests about the data.



v

How can I demonstrate that I comply?

The following Telephone Preference Service (TPS) document library illustrates how to log data policies and procedures.

Case study: how to document information

The log provides an easy framework for regular reviews and updates by the management team, driving accountability from the board down.

The document log is structured to account for the following key areas:

- Governance – policies and procedures, management structures, information risk management and compliance and assurance
- Records management – storage and maintenance of records, and disposal of records
- Security of personal data – physical security, asset management, supplier relationships, incident management and business continuity
- Data sharing – disclosures, assessing legality, risk and benefits (Data Protection Impact Assessments), informed decision making, and information sharing agreements and logs
- Training – monitoring, reporting and training programmes.

TPS Documentation Log
Spencer Wright
Date: 26/05/2017

TPS Document Log - May 2017

Id	Document Name	Area
D1	3rd Party Supplier Management Policy & Process	Compliance
D2	Access Control Policy	Compliance
D3	Business Continuity	Compliance
D4	Complaints Policy	Compliance
D5	Data Breach Notification Procedure	Compliance
D6	Data Breach Notification to the Supervisory Authority Form	Compliance
D7	Data Breach Register	Compliance
D8	Data Inventory/Information Asset Register	Compliance
D9	Data Protection Policy	Compliance
D10	Data Retention/Erasure Policy	Compliance
D11	Data Sharing Policy	Compliance
D12	Information Security Policy	Compliance
D13	Third party DPA/Information Security Questionnaire	Compliance
D14	Overall framework document	Compliance
D15	Privacy Impact Assessment Procedure	Compliance
D15b	Privacy Impact Assessment Process	Compliance
D16	Risk Assessment Framework	Compliance
D17	Schedule of Authorities and Key Suppliers	Compliance
D18	Staff Training Policy and Log	Compliance
D19	Subject Access Request Procedure	Compliance
D20	Subject Access Request Form	Compliance
D21	Complaints Acknowledgement letter to Consumer	Admin
D22	Dealing with unwanted telesales calls - FAQ's	Admin
D23	Example of a response to a complaint from a company	Admin
D24	Letter of Complaint to Company	Admin
D25	TPS Complaints Volume	Admin
D26	TPS Operational Report_May 2017	Admin
D27	TPS Policy Document - Draft	Admin
D28	What to do with unwanted calls - Complaints Form	Admin
D29	TPS Induction Slide	Corporate
D30	TPS Licence Price List	Corporate
D31	DMA Staff Handbook	HR
D32	Staff Employment Contract	HR
D33	Draft - IT Policy update	Information Security
D34	ICO users with access to TPS complaints data	Information Security
D35	ICO users with access to TPS Registration Data - (number look up)	Information Security
D36	List of companies with whom TPS shares complaints Data	Information Security
D37	TPS File Licence Agreement	Legal - Client
D38	DQM T's&C's for Consultancy Services	Legal - Supplier
D39	DMA_Telephone Preference Redesign Document	Technology

Data Protection Impact Assessments (DPIA)

DPIAs (also known as Privacy Impact Assessments or PIAs under the current law) are tools designed to help organisations assess privacy risks where the processing may incur a high risk to individuals' rights and freedoms, and when to mitigate those risks or cease the processing if the risk is too high.

An effective DPIA allows organisations to identify and fix problems at an early stage, reducing associated costs and potential reputational damage.

While not a legal requirement under the Data Protection Act, DPIAs will be in certain circumstances under the GDPR. The ICO has encouraged the use of DPIAs as an integral part of taking the approach of data protection by design.

Below are insights into making sure your organisation is fully prepared, covering:

- Data protection self-assessment toolkit:
  https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/

Use the checklist to assess your compliance with the GDPR and find out what you need to do.

Good information handling makes good business sense, and provides a range of benefits.

You'll enhance your organisation's reputation, increase customer and employee confidence and - by ensuring that personal information is accurate, relevant and safe - save both time and money.

- Data protection assurance

Recommended for first-time users. Assess your high-level compliance with the Data Protection Act.

This includes registration, fair processing, subject access, data quality, accuracy and retention.

- Getting ready for the GDPR

Designed to help you get your house in order, ready for the new legislation. It includes getting to grips with the new rights of individuals, handling subject access requests, consent, data breaches and designating a data protection officer

- Information security

Assess your compliance with data protection in the specific areas of information security policy and risk, mobile working, removable media, access controls and malware protection.

- Direct marketing

Assess yourself in the areas of consent and bought-in lists, and telephone, electronic and postal marketing.

- Records management

Records management policy and risk, record creation, storage and disposal, access, tracking and off-site storage.

- Data sharing and subject access

Sharing policy and agreements, compliance monitoring, maintaining sharing records, registration and subject access process.

When do I need to conduct a Data Protection Impact Assessment (DPIA)?

Your organisation must carry out a DPIA when:

Using new technologies

- A new analytics tool
- Using AI to assist with marketing or distribution of ads.

The processing is likely to result in a high risk to the rights and freedoms of individuals

- Use of special categories of personal data, such as health-related information, religious beliefs or marketing to children
- Profiling that may have legal effects such as differential pricing.

Processing that is likely to result in a high risk includes (but is not limited to):

- Processing activities, including profiling, where decisions have legal effects, or similarly significant effects, on individuals
- Processing of special categories of data or personal data that relates to criminal convictions or offences. This includes large-scale processing of personal data at a regional, national or supranational level, affecting many individuals and involving a high risk to rights and freedoms based on the sensitivity of the processing activity
- Data processing that has legal effect could include the use of medical or ethnic personal data (sensitive personal data). The use of such data for a marketing campaign would require both explicit consent and a DPIA
- Situations where there is systematic monitoring of publicly accessible areas on a large scale.

What information should the DPIA contain?

- A systematic description of the processing
- The purposes, including - where applicable - the legitimate interests pursued by the controller
- An assessment of the necessity and how proportional the processing is in relation to the reason for the processing
- An assessment of the risks to the rights and freedoms of individuals
- Measures to address risk, including security, and to demonstrate that you comply with the GDPR
- A DPIA can address more than one project.

The Article 29 Working Party has also published guidance on DPIAs:
http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

Data Protection Officer (DPO)

One of the biggest changes as a result of the GDPR is the creation of a specific role called the Data Protection Officer (DPO).

The DPO must report to an organisation's board and be commercially independent.

A DPO will be the customers' champion within a business, responsible for the intersection between the organisation, the customer and the regulator. Marketers should become the DPO's ally, enabling them to have an appropriate understanding of the rights and freedoms of individuals in a marketing context.

A DPO will make sure that the business is appropriately advised about how to look after customer data; that accountability can be shown in relation to the principles of the GDPR; and that your business follows the best practice outlined by the DMA Code's principles.

A DPO will ensure that the business correctly looks after customer data, accountability protocols are followed so that data is secure, and the organisation follows the best practice outlined by the DMA Code's principles, and other regulatory guidance from the ICO and Article 29 Working Party (which will become the European Data Protection Board).

GDPR states you must appoint a Data Protection Officer (DPO) if you:

- Are a public authority (except for courts acting in their judicial capacity)
- Carry out large-scale systematic monitoring of individuals, for example online behaviour tracking
- Carry out large-scale processing of special categories of data, or data relating to criminal convictions and offences

It's estimated that an additional 28,000 new Data Protection Officers will be needed across Europe by May 2018

Tasks carried out by the DPO

The DPO's tasks are defined in Article 39 of the GDPR, to:

- Inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- Have policies and procedures in place to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments, training staff and conducting internal audits
- Be the first point of contact for supervisory authorities such as the ICO and for individuals whose data is processed, like employees, customers etc.

Employer commitments to the DPO

As a business you must make sure that:

- The DPO reports to the highest management level of your organisation i.e. the board
- The DPO operates independently and is not dismissed or penalised for performing their task
- Adequate resources are given to allow DPOs to meet their GDPR obligations

Can the DPO role be given to an existing employee?

Yes - as long as the employee's duties are compatible with the duties of the DPO and do not lead to a conflict of interest. Many businesses that already have a data protection employee in place are likely to make them the DPO by default.

It will also be possible to sub-contract the role of DPO to a consultant or specialist support businesses.

Does the DPO need specific qualifications?
The GDPR does not specify the precise credentials a DPO should possess, but they should have professional experience and knowledge of data protection law.

This should be proportionate to the type of processing your organisation carries out, taking into consideration the level of protection the personal data needs to have.

If you do not employ a DPO then you should document your reasons for not doing so.

Records of processing activities (documentation)

The second big change under GDPR applies to businesses with more than 250 employees. As well as your obligation to provide comprehensive, clear and transparent privacy notices, you must maintain additional internal records of your processing activities.

Meanwhile, if your organisation has fewer than 250 employees you will also have to keep records of activities that may pose a risk to data subjects, which may include:

- Processing personal data that could result in a risk to the rights and freedoms of an individual
- Processing special categories of data or criminal convictions and offences
- Processing that is not occasional.
- Interpretation of this could change depending on the opinion of the Article 29 Working Party.

The following categories are defined as special categories of personal data:

- Racial origin
- Ethnic origin
- Political opinions or affiliations
- Religious or philosophical beliefs
- Trade union membership
- Data on health, sex life or sexual orientation
- Genetic data
- Biometric data processed to uniquely identify a person.

What do I need to record?

You must keep records of processing activities, documenting the following information:

- The name of your organisation, its registered address, company number and other relevant information, including - where applicable - the data controllers, your representative and your Data Protection Officer
- The purposes of the processing
- A description of categories of individuals and categories of personal data
- Categories of recipients of personal data
- Details of transfers to third countries including documentation of the transfer mechanism, recipients in third countries or international organisations and the safeguards used
- Retention schedules: how long do you keep data?
- A description of technical and organisational security measures.

Conclusion

Many organisations will need to make fundamental changes to update internal business processes. The demonstration of your compliance will be critical.

Compliance with GDPR is not just about buying a new IT system or adding a new training module to the HR process. If your business is already compliant with the 1998 Data Protection Act and working in line with the DMA Code, it is already halfway to becoming GDPR compliant.

Once you understand and accept the accountability elements of the GDPR, you will be in a stronger position to adapt, evolve and find it easier to respond to issues from May 2018.

Companies that build a culture with accountability at their core show a clear intent to be GDPR compliant and can expect a more collaborative approach from the ICO, should challenges arise.

The ICO has elevated the importance of accountability and made it a priority.

Assuming organisations take this on board, we will move towards a landscape where brands truly place their customers first, genuine and transparent value exchanges occur, and both business and consumer are equally protected.

Case study – A UK charity case

Overview

The CEO of a UK charity led a project to audit its level of compliance and accountability.

The organisation was keen to ensure that its current compliance met 1998 DPA standards and understand what was needed to make it GDPR compliant.

There are some unknowns: for example the charity wanted explicit consent from donors but was wary of how to do this without losing them.

Gaps were found, given a priority and presented back to the board as a plan of improvements.

This plan, once signed off by trustees, the CEO and directors, became a scope of work for the teams to implement.

The charity worked with each team to review policy statements, recruitment process and management of staff data, the security of the building, and data and IT contracts, among other things.

Steps taken

Support

The charity used supporting material from the ICO, which offers a number of useful tools on its website to help with the initial audit, including its self-assessment tool. This explores how data compliance is applied to business processes, data security and marketing consent, among other things.

Buy-in

To complete self-assessment, buy-in is needed from all teams across the business, along with a remit from the CEO and his or her direct reports. If the ICO knows a business is working towards compliance, it would likely look more favourably on them if an issue were found.

Actions

Initial meetings with wider business and marketing functions are crucial to understand what data is held, how old it is, how accurate it is likely to be, how it was captured and under what circumstances. All policy statements read and signed by staff as part of their job must be reviewed to check their compliance. The result of this self-assessment exercise is to show areas or gaps in compliance. You must document the actions you've taken to ensure compliance. You should also consider evidence from any Legitimate Interest Assessments.

In conclusion

GDPR runs throughout an organisation. It touches every department and every person's role.

Adapting to change is a big challenge for all charities. In this case, the organisation was working towards a solution which will at least test an approach.

GDPR Glossary

The GDPR uses terminology that marketers may not be familiar with. In order to provide clarity, the DMA has translated these legal terms so that marketing teams – the ones who will be implementing the changes the GDPR requires – not just legal teams can fully understand the language used.

Anonymous data: The process of removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous.

Consent: According to the GDPR, consent, "means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Controller: The organisation or individual that determines how the personal data is processed.

Legitimate interest (LI): A legal ground that can be used to process personal data for direct marketing in certain circumstances. As well as providing the right for individuals to object to the processing of personal data based on LI, the GDPR sets out strict criteria for organisations that seek to rely on LI. These include establishing that the processing is necessary and that a balancing test has been conducted.

Personal data: Any information that can be used to identify a person is personal data. For example, names and email addresses are personal data because they reveal someone's identity. The GDPR expands the definition of personal data to include IP addresses and online identifiers, like cookies.

Personal data breach: A breach of security that means unauthorised individuals or groups are able to access personal data. This could be the result of hacking by outside groups or because an employee made a mistake.

Data-protection-by-design: Data-protection-by-design is a new concept introduced by the GDPR, whereby an organisation considers what impact a particular campaign or product may have on privacy from the very start. In a marketing context this means identifying a campaign's risk for privacy and/or data protection, recording them and taking appropriate steps to mitigate them, thinking about privacy from the start and not as an afterthought.

Data-protection-by-default: Similar to data-protection-by-design, this phrase refers to privacy settings on a good or service. For example, when a phone app goes to market it should have its privacy settings set to the highest level possible as the default setting. The user could then decide to lower the privacy settings, if they so wished.

Processing: Any operation conducted on personal data, which may include collecting, recording, storing, structuring, organising, transmission or dissemination of personal data.

Processor: The organisation that only processes personal data according to the instruction of the data controller. For example, an email services organisation only processes personal data in line with what their client tells them and this means they're a data processor.

Profiling: Any type of automated processing of personal data that evaluates the characteristics of someone in order to make a decision. Marketing segmentation or targeting is a type of profiling.

Pseudonymisation: A method of making personal data no longer attributable to an individual, without further information, meaning someone could not be identified from the data. It is a process that reduces the privacy risks for people as they can no longer be identified.

Special categories of personal data: Criteria of personal data that are subject to stricter requirements because of its sensitive nature. The GDPR lists the following as special categories of personal data: "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

Supervisory authority: An independent public authority responsible for enforcing the GDPR. The Information Commissioner's Office (ICO) are the supervisory authority in the UK.

Third party: Any organisation or individual that is not the data controller or processor that is authorised by either the controller or processor to process personal data. For example, if an organisation sold personal data to another organisation, the organisation purchasing the personal data would be classed as a third party.

About the DMA

A DMA membership will grow your business.

Our network of more than 1,000 UK companies access research, free legal advice, political lobbying and industry guidance. DMA members connect at regular events that inspire creativity; showcase innovation; examine and provide insights from award-winning campaign work; and grow our understanding of how responsible marketing and the GDPR will transform how we all work.

Membership of the DMA acts as a badge of accreditation and we provide expert-led guidance across channels, underpinned by a code that puts the customer at the heart of everything we do.

We represent a data-driven industry that leads in creativity and innovation: a sector that attracts the brightest minds, the individuals that will shape the future.

By sharing our knowledge, together, we'll make it vibrant.

Find out what we can do for you: membership@dma.org.uk

About our partners

The Data Protection Network is an online community dedicated to providing expert opinion, quality resources, informative events and learning materials, to both experts and non-experts in the field of Data Protection and Privacy.

dpnetwork.org.uk

ISBA represents the leading UK advertisers. We champion the needs of marketers through advocacy and offer our members thought leadership, consultancy, a programme of capability and networking.

We influence necessary change, speaking with one voice to all stakeholders including agencies, regulators, platform owners and government.

Our members represent over 3000 brands across a range of sectors. Over a hundred members are represented on our Data Action Group, which provides discussion, events and guidance on GDPR.

ISBA is a member of the Advertising Association and represents advertisers on the Committee of Advertising Practice and the Broadcast Committee of Advertising Practice, sister organisations of the Advertising Standards Association, which are responsible for writing the Advertising Codes.

We are also members of the World Federation of Advertisers. We are able to use our leadership role in such bodies to set and promote high industry standards as well as a robust self-regulatory regime.

isba.org.uk

Copyright and disclaimer