Tuesday 24 January
@DMA_UK #dmaevents

Responsible Marketing Update: Legitimate Interest

Responsible Marketing

Sponsored by

OneTrust

Data & Marketing Association

Tuesday 24 January
@DMA_UK #dmaevents

Welcome

Chris Combemale, CEO, DMA

Sponsored by

OneTrust

DMA
Data & Marketing Association

Tuesday 24 January
@DMA_UK #dmaevents

Public Affairs and Legal Update

Chris Combemale, CEO, DMA

Sponsored by

OneTrust

DMA
Data & Marketing Association

Tuesday 24 January
@DMA_UK #dmaevents

Unlocking the Benefits of Soft Opt-In

Matt Radford, Vulnerability Consultant, Vulnerable Paths [He/Him]

Pete Meacham, Fundraising and Marketing Compliance Manager, Macmillan Cancer Support [He/Him]

Sponsored by

OneTrust

DMA
Data & Marketing Association

Charities

- There to directly benefit society.
- Support the people most disadvantaged within society.

Who Charities communicate with

- The Public
- Supporters
- Campaigners
- Activists
- Service Users
- Other Organisations and Businesses
- Etc.

Charity (marketing) communications

- Campaigning
- Fundraising
- Stewardship and Engagement
- Service and Service updates
- etc.

To Benefit

Many charity communications are sent because they can (and do) benefit people.

- Help provide **support** - Now or in the future
- **Empowering** people - With knowledge, choice or information
- Improve **wellbeing** - Give positive stories of success and change
- Give **opportunities** - To act in line with values

Consent requires a (significant) effort

- There is an effort to understand what specifically is being signed up to.
- People may not be subject specialists.
- There is effort required to actively provide consent (through forms, face to face or whatever means).

Legitimate interests requires less effort

- There remains an effort to understand what they might receive.
- Effort required to ‘not opt out’ can be understood as low.

‘Affecting the most disadvantaged’

- When there is more effort or acts required to do something, nomatter how few or small - this is most likely to affect those poorest in resource.
- The people poorest in resource are the people most likely to need support.
- More people are able to get access when things require less effort
- Consent and legitimate Interest both offer ‘opting out’, giving control and protection.

Emergencies

- Charities operate during Emergencies to help support the people affected.
- Emergencies create unforeseen changes in our environment or society which people might not have been able to reasonably foresee or prepare for.

Emergencies and consent

- Specific types of consent may not give permission for sharing valuable information.
- Reconsent or additional consents are examples of further resource loads placed on people.
- This is done when they are likely to have negatively impacted resources.

Emergencies and Legitimate Interest

- Legitimate Interests supports sending information which is in the interests of the recipient.
- This is without additional effort by the recipient.
- The ability to opt out continues to remain.

‘Supporter first’ approach

Being able to use legitimate interest can mean more people have a chance to receive more relevant help, support and empowerment.

Implementing Soft Opt-in Responsibly

MACMILLAN CANCER SUPPORT

Our Supporter Promise

You can expect;

"To choose how we contact you and change this at any time".

"To not feel under pressure to give more or more frequently than you want".

We promise;

"We'll use your details in the way you have agreed to and only tell you about things we think you may be interested in".

MACMILLAN CANCER SUPPORT

Using Soft Opt In Responsibly

- Due Diligence
- Transparency
- Set Parameters
- Opt Outs

MACMILLAN CANCER SUPPORT

In Conclusion……

MACMILLAN CANCER SUPPORT

Tuesday 24 January
@DMA_UK #dmaevents

Applying Legitimate Interest in Advertising Mail

Andrew Bridges, Data Governance Manager, Sagacity

Sponsored by

OneTrust

Data & Marketing Association

UK GDPR changed everything …as it should have

Permissions

Responsibility

Transparency

Accountability

UK GDPR – The Basics

What is the UK GDPR and or DPA 2018 are they the same thing?

The Data Protection Act 2018 controls how **your** personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

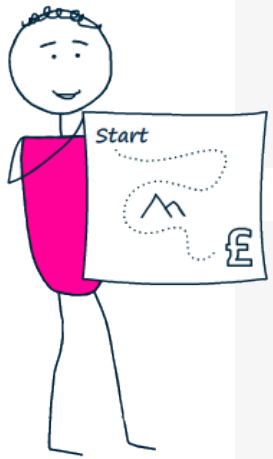
What does the UK GDPR cover?

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals.

Who enforces UK GDPR?

The Data Protection Act 2018 controls how **your** personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

The 7 Guiding Principles



- Accuracy
- Data minimisation
- Storage limitation
- Accountability
- Lawfulness, fairness and transparency
- Purpose limitation
- Integrity and confidentiality (security)

Purpose Limitation Under UK GDPR

The purpose of processing personal data must be planned and defined clearly before the start of processing. Personal data may only be collected and processed for a specific and lawful purpose. **The data may not be processed in a manner inconsistent with the original purpose at a later date**.

Art. 5 UK GDPR Principles relating to processing of personal data

1.Personal data shall be:

(a)processed lawfully, fairly and in a transparent manner in relation to the data subject ('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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

Lawfulness of Processing

- What does each lawful basis mean?
- Why is it needed, why does an organisation need to choose a lawful basis?
- Hierarchy of lawful basis
- How to apply a lawful basis (i.e if you ask for consent you cannot choose another if not accepted)
- What lawful basis do we use to process data, is it different per channel and why?

What Does Lawfulness of Processing Mean?

Under the UK GDPR usage of personal data is limited to a stated purpose and legal ground.

All processing of personal data you undertake should be documented in a GDPR register along with its purpose and legal basis.

The law provides six legal bases for processing: consent, performance of a contract, a legitimate interest, a vital interest, a legal requirement, and a public interest.

UK GDPR requires any organisation processing personal data to have a valid legal basis for that processing activity.

Lawfulness of Processing

Processing is only lawful when at least one of the following applies

01
Contract

The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

02
Legal Obligation

The processing is necessary for you to comply with the law (not including contractual obligations).

03
Legitimate interest

You or a third party have a legitimate interest that makes processing the data necessary, and there are no other individual's interests, rights or freedoms that outranks your interest. For example, you might have a legitimate interest in marketing your goods to existing customers to increase sales.

04
Consent

The individual has given clear consent for you to process their personal data for a specific purpose.

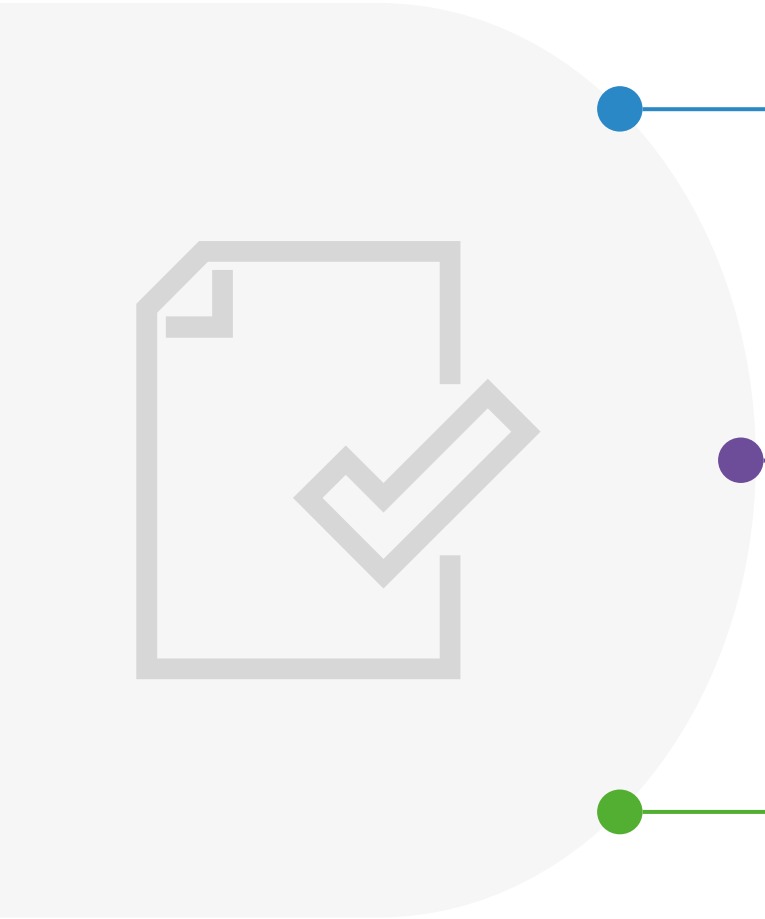
05
Vital interest

The processing is necessary to protect someone's life, e.g., in an emergency situation.

06
Public interest

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

What should you consider before you choose a Lawful basis … how do you decide?



You **must** have a valid data protection reason, if you want to use people's information for your direct marketing activity (known as a "lawful basis").

You **must** choose which is the most appropriate, depending on your direct marketing activity, the context and your relationship with the person.

In general, consent and **legitimate interests** are the two lawful bases most likely to apply to your direct marketing.

Special Category Data… What is it and how can it be processed under UK GDPR?

Art 9-1

Processing of personal data revealing 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 shall be prohibited.

Art 9-2 (a)

The data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.

Hierarchy of Lawfulness

Does anybody want to guess?

How to Apply a Lawful Basis, i.e. If You Ask For Consent, You Cannot Choose Another if Not Accepted

Challenge 01

The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

Challenge 02

Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason. Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.

Challenge 03

If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).

Challenge 04

If you are processing special category data, you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

And its Worth Remembering… Direct Marketing has always been ‘opt out’ - No change from the DPA 98

Legitimate Interest

Legitimate Interest does not require an organisation to be named at capture as long as you can show consumers would reasonably expect the data to be used in a way that has a minimal privacy impact, essentially good practice is to name sector and a descriptive list of sectors in your privacy.

Consent

Consent **does** require an organisation to be named at capture and is ‘opt’ in, collected unbundled and should never be pre-ticked i.e., consent requires a positive /affirmative action to be recorded

Direct Marketing Guidance…What Does the Regulator Say?

> You **must** tell people that you want to collect and use their information for direct marketing purposes. You **must** be clear about what you want to do and your privacy information **must** be easy for people to understand.
>
> Getting new information about people from other sources or by profiling their interests and habits can help target your direct marketing more effectively. But you **must** ensure that doing this is fair and tell people about it.

Let’s Expand on What Should You Tell Individuals

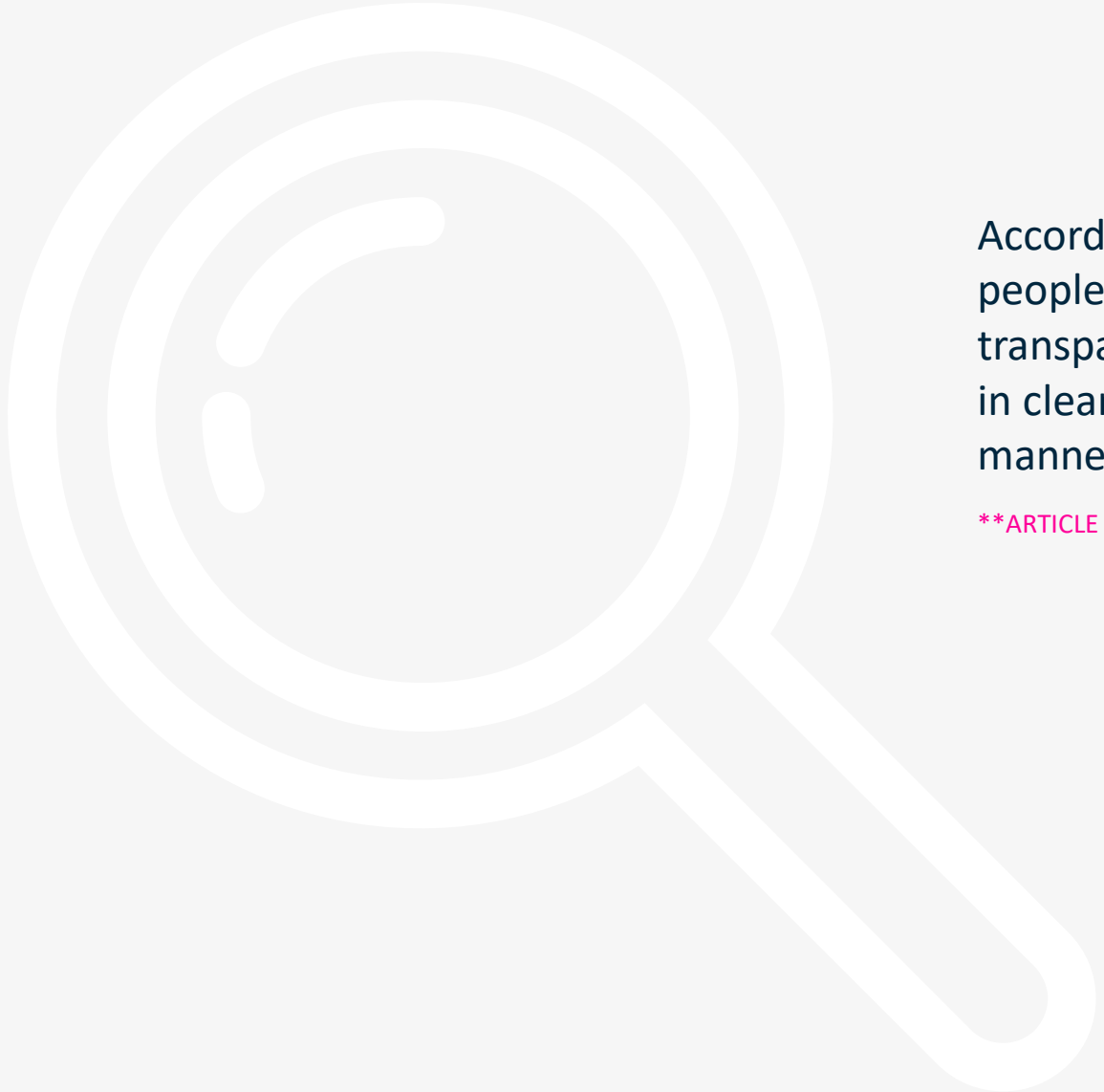
- Explain why you want to use their information (eg to send postal marketing, to profile their buying habits);
- Tell them if you intend to share their information with other organisations for direct marketing purposes; and
- Make them aware of their data protections rights (including the right to object to direct marketing).

You **must** provide this privacy information to people at the time you collect their details. If, at a later date, you want to use the information for other activities, you **must** give them further privacy information (assuming the new things you want to do are fair and lawful).

Your privacy information **must** be in clear and plain language. It **should** be easy for people to understand what you are saying to them. You **should** tailor it to your audience (eg who are your customers and what are they likely to understand?) and use language and terms they will be familiar with and will understand. If you find it difficult to explain what you want to do, or you don’t want to tell people because you think they might object, this is a sign that you **should** rethink your intended marketing activity.

There is no set way to provide your privacy information. The method depends on your audience and the way you collect the information (e.g. online, over the phone, by post)

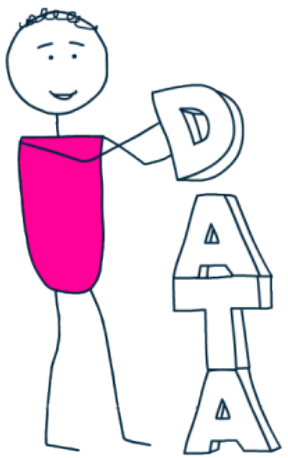
What Needs to be in a UK GDPR Privacy Policy?



According to the UK **GDPR**, organisations must provide people with a **privacy notice** that is: In a concise, transparent, intelligible, and easily accessible form. Written in clear and plain language and delivered in a timely manner.

**ARTICLE 29 DATA PROTECTION WP Guidelines on transparency under Regulation 2016/679

Layered Privacy Approach



**In an online context, the use of a layered privacy statement/ notice will enable a data subject to navigate to the particular section of the privacy statement / notice which they want to immediately access rather than having to scroll through large amounts of text searching for particular issues.

The requirement that information is “intelligible” means that it should be understood by an average member of the intended audience. This means that the controller needs to first.

**ARTICLE 29 DATA PROTECTION Working Party Guidelines on transparency under Regulation 2016/679

That Other Relevant Article

That Other Relevant Article - Recital 47… Check Out The Last Sentence

Recital 47

Overriding Legitimate Interest*

[1] The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. [2] Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. [3] At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. [4] The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. [5] Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. [6] The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. [7] The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

* This title is an unofficial description.

**The recitals provide additional information and supporting context to supplement the articles. The European Data Protection Board—formerly Article 29 Working Party—relies on the recitals to interpret the articles. ... Through the recitals, organisations learn when and how to comply with the GDPR.

Balancing Under UK GDPR

- What is a LIA and why should they be used?
- What is a PIA and why should they be used?
- What is a DPIA and why they should be used?

Legitimate Interest Assessment

An LIA is a three-part test which requires you to: identify your legitimate interest; show that the processing activity is necessary to achieve that legitimate interest; and. balance the processing activity against the rights and freedoms of the data subject.

Who should write one?

Privacy Impact Assessment

The objective of the PIA is to systematically identify the risks and potential effects of collecting, maintaining, and disseminating PII and to examine and evaluate alternative processes for handling information to mitigate potential privacy risks.

Who should write one?

Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project. You must do a DPIA for processing that is likely to result in a high risk to individuals.

Who should write one?

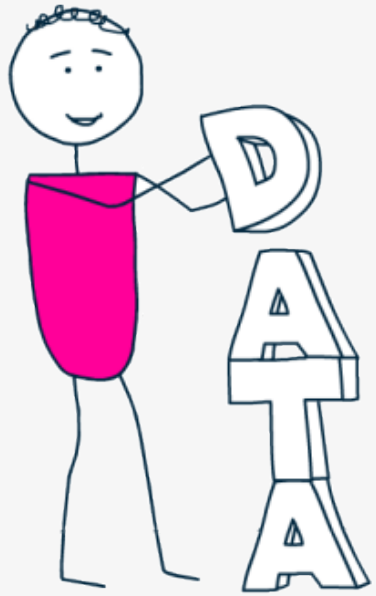
Due Diligence…What You Need to Align to the UK GDPR

Whilst the UK GDPR requires any organisation to keep personal data up to date ‘where necessary’, their processing must always be fair. The actions taken to update contact details must be reasonable and proportionate.

The overriding factor of the GDPR is the transparency of these processes, the privacy policy served to consumers at point of permission collection should be transparent and explain that organisations will be conducting these processes on the data.

Sagacity always suggest the client conducts their own balancing test and privacy impact assessments to justify the processing, whether that be prospecting , cleansing, enhancement, linking, matching and tuning.

Remembering that the fundamental rights of the consumer are protected and that the balancing is in equal measure, i.e., the legitimate interest for both client and customer is balanced, one doesn’t out way the other.



Legal and Compliance…Who Covers What and How to Work in Conjunction

A **compliance department** ensures adherence to internal controls and external rules/regulations

Legal counsel is in charge of contract drafting, negotiation, and review, defining the law which in turn dovetails with a compliance team…..

Tuesday 24 January
@DMA_UK #dmaevents

/ Ask Us Anything Legal Panel

Victoria Tuffill, Partner, Data Compliant

Pete Meacham, Fundraising and Marketing Compliance Manager, Macmillan Cancer Support

Andrew Bridges, Data Governance Manager, Sagacity

Matt Radford, Vulnerability Consultant, Vulnerable Paths [He/Him]

Sponsored by

OneTrust

DMA
Data & Marketing Association

Tuesday 24 January
@DMA_UK #dmaevents

Closing Comments

Chris Combemale, CEO, DMA

Sponsored by

OneTrust

Data & Marketing Association