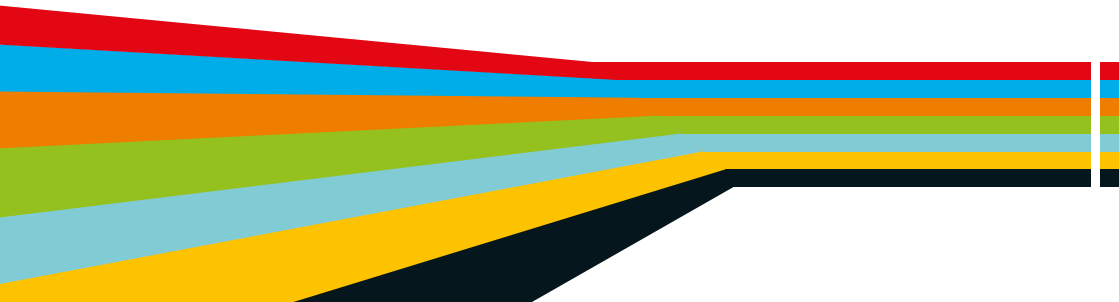
GDPR MAILWISE

Royal Mail

# THE GDPR OPPORTUNITY WITH MAIL



# CONTENTS



# INTRODUCTION TO MAIL UNDER THE GDPR

The General Data Protection Regulation (GDPR) has far-reaching implications for Royal Mail and its customers. But we are optimistic that the new data laws will have a positive impact on relationships between organisations and consumers. We believe it presents a tremendous opportunity for us all to take stock of our marketing processes and put best-quality data practices at the heart of our organisations. By encouraging greater transparency, we believe that the GDPR will provide a major impetus for us all to improve our direct marketing communications, and ensure they are always well targeted and well received.

Of course, there are understandable concerns. For instance, from conversations with our customers, we understand there's confusion about what constitutes "legitimate interests" in relation to direct marketing, when consent is necessary, and how third-party data can lawfully be used in the context of the GDPR. Our customers have also said that the guidance they've received from events and through online marketing blogs has sometimes been contradictory – even alarmist.

This guide does not impart any legal advice, but is instead designed to help organisations become acquainted with the most important sources of information on the GDPR, including what the law itself says and what the UK's data protection regulator, the Information Commissioner's Office (ICO) has, so far, decided this means. As the ICO is regularly delivering updates to its guidance on implementation, this guide serves as an introduction to some of the main subject areas with which organisations need to become familiar.

The guide also highlights the important and unique role that mail will continue to play in driving business success in a post-GDPR world. It includes examples from organisations that have already been inspired by the GDPR to improve their data practices and build more trusting, open and transparent relationships with customers.

While the journey to compliance with the GDPR may not always be an easy one, Royal Mail can provide help and support every step of the way – an assurance that we hope this guide makes abundantly clear.

**Jonathan Harman**
Managing Director
Royal Mail MarketReach

# WHAT IS THE GDPR?

The GDPR comes into force on 25th May 2018. It is not a brand new regulation, but a necessary evolution to the existing Data Protection Act. It is intended to extend additional protection for individuals and their data, providing greater transparency and control over where their data is saved and used. The ICO is working hard to produce guidance on what the new law means for organisations, and how they can become compliant. It warns that while its final guidance is compiled, no organisation should think that because the UK is leaving the EU, they do not need to plan for compliance.

**25 MAY 2018**

The ICO is committed to assisting businesses and public bodies to prepare to meet the requirements of the GDPR ahead of May 2018 and beyond. The Information Commissioner, Elizabeth Denham, has acknowledged that there "may still be questions about how the GDPR would apply in the UK on leaving the EU, but this should not distract from the important task of compliance with the GDPR."

What should also be acknowledged is the global nature of the GDPR. All EU member states will implement the GDPR and certain obligations (such as in relation to international data transfers) apply when working across borders. Furthermore, countries outside of Europe may need to comply with relevant aspects of the GDPR when trading with European countries so, from a certain point of view, the GDPR can be considered a law with implications worldwide.



# WHO DOES THE GDPR APPLY TO?

**The ICO makes clear that the new law applies to 'controllers' and 'processors' of data, and these are largely the same definitions that apply today under the Data Protection Act 1998 (DPA). A controller is responsible for how and why the data is processed, while the processor acts on the controller's behalf.**

## PROCESSORS

**The ICO GDPR guide elaborates on specific responsibilities**

"If you are a **processor**, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach."

These obligations for processors are a new requirement under the GDPR.

## CONTROLLERS

**The ICO GDPR guide, continues:**

"However, if you are a **controller**, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR. The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU."

# WHAT INFORMATION DOES THE GDPR APPLY TO?

## PERSONAL DATA

According to the GDPR, the GDPR applies to "personal data", meaning any information relating to an identifiable person who can be directly or indirectly identified, in particular, by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. The GDPR applies to both automated personal data and to manual filing systems in which personal data is accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data. Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR, depending on how difficult it is to attribute the pseudonym to a particular individual.

## SPECIAL CATEGORIES OF PERSONAL DATA

The GDPR refers to certain types of personal data - currently known as sensitive personal data - as "special categories of personal data".

The following categories of data are considered "special categories":

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade-union membership
- data concerning health or sex life and sexual orientation
- genetic data (new)
- biometric data where processed to uniquely identify a person (new)

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

## FINES

Fines under the current Data Protection Act are up to £500,000, but under the GDPR, these are set to increase to a maximum of 4 per cent of group annual global turnover, or €20 million, whichever is greater.

The Information Commissioner has gone so far as to blog to set the record straight on fines and put minds at rest. Focus should be on compliance, not speculating about fines. She suggests:

> "This law is not about fines. It's about putting the consumer and citizen first. We can't lose sight of that. It's true we'll have the power to impose fines much bigger than the £500,000 limit the DPA allows us. It's also true that companies are fearful of the maximum £17 million, or 4 per cent of turnover allowed under the new law. But it's scaremongering to suggest that we'll be making early examples of organisations for minor infringements, or that maximum fines will become the norm...
>
> ...The ICO's commitment to guiding, advising and educating organisations about how to comply with the law will not change under the GDPR. We have always preferred the carrot to the stick...
>
> ...Our Information Rights Strategy – a blueprint for my five-year term in office – confirms that commitment. And just look at our record: Issuing fines has always been, and will continue to be, a last resort. Last year (2016/2017) we concluded 17,300 cases. I can tell you that 16 of them resulted in fines for the organisations concerned...
>
> ...And we have yet to invoke our maximum powers…
>
> ...Like the DPA, the GDPR gives us a suite of sanctions to help organisations comply – warnings, reprimands, corrective orders. While these will not hit organisations in the pocket – their reputations will suffer a significant blow...
>
> ...And you can't insure against that." "

# THE GDPR KEY POINTS

## LAWFUL PROCESSING

The ICO has offered very clear guidance that to be GDPR compliant, organisations must identify which of the six legal bases for processing personal data they are using. To quote their guidance:

- "For processing to be lawful under the GDPR, you need to identify a lawful basis before you can process personal data."
- "It is important that you determine your lawful basis for processing personal data and document this."
- "Your lawful basis for processing has an effect on individuals' rights. For example, if you rely on someone's consent to process their data, they will generally have stronger rights, for example, to have their data deleted."

The GDPR allows member states to introduce more specific provisions in relation to Articles 6(1)(c) and (e), below:

- "processing is necessary for compliance with a legal obligation";
- "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."

"These provisions are particularly relevant to public authorities and highly regulated sectors."

## LAWFULNESS OF PROCESSING CONDITIONS

**Article 6(1) sets out the 6 lawful bases for processing personal data:**

(a) Consent of the data subject

(b) Processing is necessary for the performance of a contract with the data subject, or to take steps to enter into a contract

(c) Processing is necessary for compliance with a legal obligation

(d) Processing is necessary to protect the vital interests of a data subject or another person

(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

(f) Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject



# CONSENT AND LEGITIMATE INTERESTS

Of the six legal bases to process data, the ICO has provided some further information on both consent and legitimate interests.

## CONSENT

The ICO has pointed out that under the GDPR's definition of consent, there are two new points (additional to the DPA) for organisations to consider. It has highlighted these in bold when repeating the law's definition of consent:

"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."

The ICO's guide to consent provides a list which elaborates on this definition to show that, under the GDPR, consent must be:

- **Unbundled:** consent requests must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service.
- **Active opt-in:** pre-ticked opt-in boxes are invalid – use unticked opt-in boxes or similar active opt-in methods (e.g. a binary choice given equal prominence).
- **Granular:** give granular options to consent separately to different types of processing wherever appropriate.
- **Named:** name your organisation and any third parties that will be relying on consent – even precisely defined categories of third-party organisations will not be acceptable under the GDPR.
- **Documented:** keep records to demonstrate what the individual has consented to, including what they were told, and when and how they consented.
- **Easy to withdraw:** tell people they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw as it was to give consent. This means you will need to have simple and effective withdrawal mechanisms in place.
- **No imbalance in the relationship:** consent will not be freely given if there is imbalance in the relationship between the individual and the controller – this will make consent particularly difficult for public authorities and for employers, which should look for an alternative lawful basis.

## MAIL AND LEGITIMATE INTERESTS

Some organisations may wish to explore with their legal teams whether legitimate interests are a more appropriate legal basis upon which to process personal data for specific purposes, which can include direct marketing. Article 6(1)(f) in the GDPR gives legitimate interests as a lawful basis of processing where:

"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

**"YOU WON'T NEED CONSENT FOR POSTAL MARKETING"**
**ICO, 2018**

The ICO Guide to GDPR adds:

"A wide range of interests may be legitimate interests. They can be your own interests or the interests of third parties, and commercial interests as well as wider societal benefits. They may be compelling or trivial, but trivial interests may be more easily overridden in the balancing test."

## LEGITIMATE INTERESTS ASSESSMENTS

The ICO breaks down the assessments into a three-part test:

1. Purpose test: are you pursuing legitimate interests?
2. Necessity test: is the processing necessary for that purpose?
3. Balancing test: do the individual's interests override the legitimate interests?

The ICO explains "The GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list. It also says that you have legitimate interests in disclosing information about possible criminal acts or security threats to the authorities.

'Necessary' means that the processing must be a targeted and proportionate way of achieving your purpose. You cannot rely on legitimate interests if there is another reasonable and less intrusive way to achieve the same result."

"Legitimate interests is the most flexible lawful basis, but you cannot assume it will always be appropriate for all of your processing. If you choose to rely on legitimate interests, you take on extra responsibility for ensuring people's rights and interests are fully considered and protected."

The ICO then illustrates how legitimate interests can be applied in Marketing with additional reference to the Privacy & Electronic Communications Regulation (PECR) which you must adhere to where you are using electronic channels.

"You won't need consent for postal marketing but you will need consent for some calls and for texts and emails under PECR. See ICO Guide to PECR for more on when you need consent for electronic marketing.

If you don't need consent under PECR you can rely on legitimate interests for marketing activities if you can show how you use people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object."

With further additional requirements to utilise legitimate interests including:

"You must tell people in your privacy notice that you are relying on legitimate interests, and explain what these interests are."

"If you are relying on legitimate interests for direct marketing, the right to object is absolute and you must stop processing when someone objects. For other purposes, you must stop unless you can show that your legitimate interests are compelling enough to override the individual's rights."

Please refer to the ICO Guide to General Data Protection Regulation (GDPR) for more details on when you can use legitimate interests and how to apply it in practice.

## MAIL AND LEGITIMATE INTERESTS

The Data Protection Network produced a guide to legitimate interests which includes examples of scenarios in which legitimate interests would be a legal basis for processing personal data, including:

### Direct marketing

A charity sends a postal mailshot out to existing supporters, providing an update on its activities and details of upcoming events.

### Personal data transferred in an acquisition

A publisher acquires circulation data of several magazine titles in the course of a business acquisition and wishes to use the data for similar purposes to those for which it was originally acquired.

### Postal marketing from third parties

A catalogue company adds details to its online order forms which indicate that it shares data with other cataloguers. The purchaser can opt-out of this sharing, and the other cataloguers are listed in the privacy statement.

### Personalisation

A travel company relies on consent for its marketing communications, but may rely on legitimate interests to justify analytics to inform its marketing strategy, and to enable it to enhance and personalise the "consumer experience" it offers its customers.

## THE RIGHTS OF THE INDIVIDUAL

**The ICO has been very clear that implementation of the GDPR will require organisations to observe and uphold the public's strengthened data rights. It has provided a list, with brief explanations, of what these rights are:**

- **The right to be informed** encompasses your obligation to provide "fair processing information", typically through a privacy notice. It emphasises the need for transparency over how you use personal data.
- **The right of access** allows individuals the right to access their personal data and supplementary information. This enables individuals to be aware of and verify the lawfulness of the processing.
- **The right to rectification** gives individuals the right to have personal data rectified. Personal data can be rectified if it is inaccurate or incomplete.
- **The right to erasure** enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- **The right to restrict processing.** Individuals have a right to "block" or suppress processing of personal data. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.
- **The right to data portability** allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
- **The right to object** allows individuals the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.
- **Rights in relation to automated decision-making and profiling.** The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

# ICO'S 12 STEP PREPARATION GUIDE

The ICO has produced a 12-point guide to what organisations need to do to prepare for the GDPR becoming law in May 2018.

From raising awareness at every level within a company, to auditing data and establishing a legal basis for processing and storing personal information, this guide can help organisations plan for compliance.

**Preparing for the General Data Protection Regulation (GDPR)** | **12 steps to take now**

**1. Awareness**
You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

**2. Information you hold**
You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

**3. Communicating privacy information**
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

**4. Individuals' rights**
You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

**5. Subject access requests**
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

**6. Lawful basis for processing personal data**
You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

**7. Consent**
You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

**8. Children**
You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

**9. Data breaches**
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

**10. Data Protection by Design and Data Protection Impact Assessments**
You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from Article 29 Working Party, and work out how and when to implement them in your organisation.

**11. Data Protection Officers**
You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

**12. International**
If your organisation operates in more than one EU member state (i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

ico.
Information Commissioner's Office

ico.org.uk



# WHAT'S STILL TO COME?

Some of the information the ICO will be providing is dependent on guidance provided by the Article 29 Working Party.

## WHAT IS THE ARTICLE 29 WORKING PARTY?

This working party is mentioned frequently when the ICO discusses how it is shaping the GDPR compliance guidance it passes on to organisations.

To quote the European Data Protection Supervisor (EDPS): "The 'Article 29 Working Party' is the short name of the Data Protection Working Party established by Article 29 of Directive 95/46/EC. It provides the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States.

"The Working Party is composed of:

- representatives of the national supervisory authorities in the Member States;
- a representative of the EDPS;
- a representative of the European Commission."

The Article 29 Working Party also adopts guidelines for complying with the requirements of the GDPR. The ICO has explained how guidance from Article 29 is shaping its progress in providing final guidance before May 2018.

# WHAT'S HAPPENING WITH ePRIVACY, AND WHEN?

The draft EU ePrivacy Regulation was published at the beginning of January 2017, with the original intention that it should be implemented within the same time frame as the GDPR. It will update and replace the UK's Privacy and Electronic Communication Regulation 2003 (known as PECR). However, since then there have been significant delays to its progress at EU level and as a result the timescale is unclear.

The ICO has provided guidance on what the new ePrivacy Regulation is likely to mean for organisations.

The current draft proposal includes some headline changes:

- It removes separate security obligations, which will be covered under the GDPR, but introduces customer notification of specific security risks.
- In terms of cookies and other online tracking devices, the focus shifts from website cookie banners to users' browser settings, and seeks to address issues around ad-blocking and wi-fi location tracking.
- It tightens the rules on marketing, with the default position being that all marketing to individuals by phone, text or email must be opt-in.
- It incorporates the GDPR's two-tier system of fines of 4 per cent of worldwide turnover, or up to €20 million for breaches of some parts of the Regulation.
- It would apply to services providing so-called 'over-the-top' communication channels over the internet, such as Skype, Messenger or WhatsApp. It would also apply to businesses providing customer wi-fi access, as well as the traditional telecoms and internet providers.
- It would apply to organisations based anywhere in the world if they provide services to people in the EU."

## USEFUL RESOURCES

This is a selection of some of the most useful resources currently available. Please note these are subject to change.

1. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

   This is a living document and the ICO is working to expand it in key areas. It includes links to relevant sections of the GDPR itself, to other ICO guidance, and to guidance produced by the EU's Article 29 Working Party.

2. https://www.dpnetwork.org.uk/gdpr-10-point-checklist-marketers/

3. https://dma.org.uk/gdpr

4. https://dma.org.uk/uploads/misc/58f881147dcd0-gdpr-checklist-copy_58f881147dc1e.pdf

5. https://www.dpnetwork.org.uk/dpn-legitimate-interests-guidance/

6. https://dma.org.uk/article/10-things-marketers-need-to-know-about-the-gdpr

7. https://ico.org.uk/media/about-the-ico/documents/1624382/ico-annual-track-2016.pptx

# THE GDPR OPPORTUNITY

New regulations can initially seem a little daunting in any industry, and the GDPR will certainly require organisations to examine how they process and use customer data. However, it also presents an opportunity to create relationships with customers and prospects that are more transparent and trust based.

## TACKLING DISTRUST

The 2016 Annual Tracker study by the ICO showed that UK adults had "little confidence" in the current state of the data economy, and that a "data-sharing tension" existed between consumers and businesses over privacy protection. Consumers are concerned that by handing over personal information, they run the risk of having their private information stolen by criminals, receiving nuisance calls and spam, or having their data sold on to third parties for marketing purposes without their knowledge.

Only 3 per cent of the British population are currently unconcerned about sharing personal information, and only one in five thinks the current law, the Data Protection Act, is sufficient to protect them. Just 15 per cent believe the individual is in control of their personal information.

The GDPR seeks to allay this distrust, and as such, it presents an opportunity for marketers to build improved relationships with their customers and prospects by positively embracing the new powers that the law gives consumers.

## A BRAND DIFFERENTIATOR

The GDPR provides an opportunity for organisations to truly embrace data protection as a brand differentiator – a core value that engenders better, more trusting relationships with consumers.

These transparent relationships, in which brands are respectful of privacy and data protection, enable organisations to be more upfront and honest about what information they would like to receive from a customer or prospect, and what they intend to do with it.

Organisations can use the GDPR as a fundamental building block to improve trust with consumers and create a permission pathway that delivers a better view of each customer as an individual.

## BUILDING BETTER RELATIONSHIPS

The Direct Marketing Association (DMA) has outlined the top 10 key areas organisations need to be aware of in implementing the GDPR which, it claims, can also be seen as "business benefits". These are:

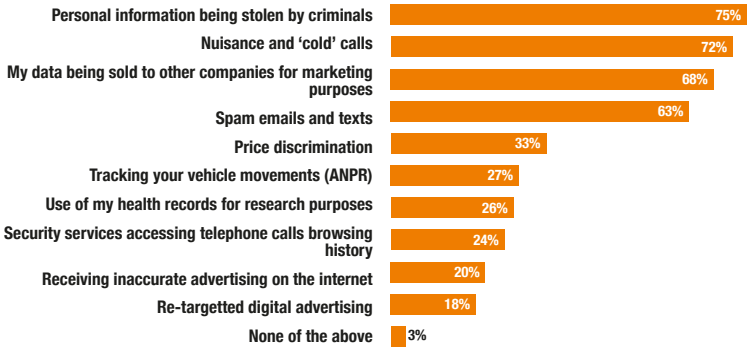
- **Business transformation:** The GDPR is a watershed moment for companies to make data protection a core brand value.
- **Respecting privacy:** Respecting privacy is central to the future of customer relationships.
- **Accountability** is a core principle: The GDPR asks companies to be accountable for their own decisions on how they collect and use personal data.
- **Total responsibility across your business:** Accountability applies to everyone.
- **Accountability goes right to the top:** Accountability should be driven at board level – it's not just an issue for the lawyers.
- **Training is vital:** It is important people working within companies are trained as to what their responsibilities are.
- **Privacy is a key ingredient:** Privacy should be baked into every product from the beginning.
- **The customer must benefit:** Transparency means telling the customer what you are going to do with their data and the benefits they get in return.
- **If trust is lost, all is lost:** It is necessary to build trust in the digital economy.
- **Build for the future:** Being open, honest and transparent about what you are going to do with your customers' data is good for loyal, sustainable customer relationships.

# THE ICO RUNS AN ANNUAL TRACKER REPORT INTO CONSUMER ATTITUDES TO SHARING DATA WITH ORGANISATIONS

**The 2016 study noted popular consumer fears about what might result from sharing data.**

## UK adults fear their personal data being sold for marketing almost as much as it being stolen.

**Most concerning use cases of personally identifiable information.**




**There were four main concerns:**

**75%** Private information is being stolen by criminals

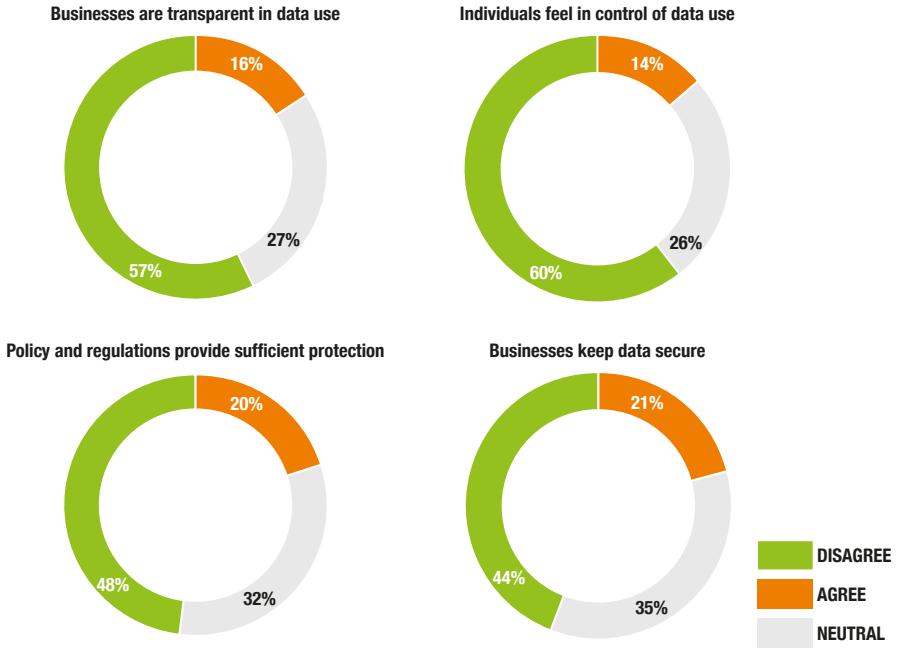
**72%** Nuisance and 'cold' calls

**68%** Data being sold on to third parties for marketing purposes

**63%** Spam emails and texts

Q12 Which, if any, of the following outcomes are you most concerned about when businesses use your personal information? DPA Survey Base: All UK adults (n=1249)

## UK adults have little confidence in the current state of the data economy.




**The study also showed:**

**57%** Do not believe companies are transparent in their use of data

**48%** Do not believe the DPA is sufficient to protect them

**60%** Do not believe individuals have control over their personal data

**44%** Do not believe companies do enough to keep their data safe

Q11A Businesses are open and transparent about how they collect and use my personal information DP Base: All UK adults (n=1249) 18-24 (n=144)
Q11B You have lost control over the way your information is collected and used by companies [scale flipped for ease of reading] DP Base: All UK adults (n=1249)
Q11C Existing laws and organisational practices provide sufficient protection of your personal information DP Base: All UK adults (n=1249) Baby Boomers (n=388)
Q11D Online companies collect and keep your personal details in a secure DP Base: All UK adults (n=1249)

# 12 WAYS MAIL COULD HELP YOU THRIVE IN A GDPR WORLD

**Marketers are embarking on the biggest regulatory change we have seen in our working lifetimes.**

Whilst it's good news for customers and good news for our industry, it is going to force some change on us. And as we all review our marketing models and channel choices, we'd like to suggest a number of reasons that direct mail could be part of the way you ensure success in a GDPR world.

## 1. YOU WON'T NEED CONSENT FOR POSTAL MARKETING

Quoting from the ICO website, "You won't need consent for postal marketing but you will need consent for some calls and for texts and emails under PECR." This means that brands may have some customers they can only reach by mail because mail is still subject to fewer regulations than electronic communications.

## 2. BRANDS WILL HAVE FEWER REGULATORY UNKNOWNS.

Brands will have fewer regulatory unknowns when contacting by mail than by electronic channels. Mail is not materially impacted by the proposed ePrivacy Regulation, whereas electronic channels are. The ePrivacy Regulation was scheduled to come into effect in May 2018 but given there is no timetable for finalising the draft, this deadline is looking increasingly unrealistic leaving a number of questions unanswered.

## 3. MAIL IS RECOMMENDED BY THE DMA TO GET CONSENT.

Mail is recommended as the channel to use to get consent by the DMA. Some brands will choose to repermission some customer segments, and mail is well suited to this. Brands have been fined for contacting customers by email who had previously opted out of email communication. Repermissioning communications are seen as marketing activity, and so mail of this nature can attract advertising mail discounts.

## 4. MAIL OFFERS HIGHER RESPONSE RATES THAN EMAIL.

In a world where trust and frequency of communication are increasingly important to manage, mail is welcomed by recipients and offers higher response rates than email.* Consumers recognise that mail takes more effort than email. So when it is used, it reassures them that companies recognise and value them – they cared enough to send mail.

## 5. NO FINES AS YET FOR USING MAIL FOR MARKETING.

No one has been fined by the ICO for using mail for marketing. According to the ICO website, seventeen penalties were issued in 2017 for other channels, such as text, phone calls and email.

## 6. IT'S EASY TO STAY IN TOUCH VIA MAIL.

While people are more likely to have multiple email addresses, including ghost ones they do not check, people generally only have one residential postal address, and our home-mover data services make it possible to stay in touch if your customer moves.

* US Data & Marketing Association Response Rate Report 2017

# 12 WAYS MAIL COULD HELP YOU THRIVE IN A GDPR WORLD

## 7. DON'T FORGET THE POWER OF UNADDRESSED MAIL.

Not everyone will grant consent via a repermissioning exercise. Door drops offers targeted services that are delivered with addressed mail that enables you to re-engage these audiences without using personal data. Door drops is an area of increasing innovation around targeting and price points. Research shows unaddressed items stay in the home for an average of 38 days and are frequently revisited. Be sure to talk to us about how we can help.

## 8. MAIL PRIMES OTHER MEDIA.

Our Private Life of Mail neurological study proved the way that mail primes other media. So you may expect email and other electronic communication to be better recognised and received (and perhaps unsubscribe rates to be lower) if the recipient has been mailed in the weeks before.

## 9. MAIL HAS EVOLVED.

It may be 500 years old, but mail continues to evolve. In recent years we have introduced programmatic mail and barcodes on mail to enable message sequencing, and in 2018 JICMAIL will launch to provide reach and frequency data to the market.

## 10. WE CAN HELP YOU KEEP YOUR DATA CLEAN.

Article 5 of the GDPR means that businesses will be held accountable for the accuracy of their customer data. Royal Mail has the leading industry update and suppression files which are fully GDPR ready. Accurate data will help you improve the return on investment of your mail campaigns.

## 11. WE CAN HELP YOU TO DEPLOY YOUR NEXT MAIL CAMPAIGN.

We have a comprehensive team of Media Specialists and media and data planners that can help you. We also have hundreds of case studies, insight, tools and data planning support to help you get the most from your investment in mail. It's all free of charge to mail users.

## 12. WE'LL PUT OUR MONEY WHERE OUR MOUTH IS.

We can often offer a price incentive to encourage you to invest more in mail or try a different use of mail. Whether you're new to mail, repermissioning, testing new data, or door drops, call us to see what we can do.

# CASE STUDY 1:
# CANCER RESEARCH UK

## CANCER RESEARCH UK NEEDED "ONE TICK" TO BEAT CANCER SOONER

**With the spotlight on charity fundraising practices, in 2016 Cancer Research UK took the bold decision to change to an "opt-in" model for marketing. This was a decision driven primarily by the desire to change the way it talked to supporters, and one that the charity hoped would put it in a good position once the GDPR's requirements were announced later in the year.**

### A PHASED APPROACH WAS USED TO DELIVER THE CHANGE

It meant that the charity chose only to contact supporters with marketing activity, who had provided explicit consent to be contacted via that communication channel.

A phased approach was used to deliver the change, initially prioritising updating data-capture forms from new or returning supporters by the end of May 2016. The charity became opt-in for all supporters on 1 July 2017.

A major campaign kicked off the opt-in drive. Launched in the Sunday Times it spread across press, mail, social media, YouTube advertising and PR. The message was clear, 'Your Tick Beats Cancer Sooner'.

**In the first three months of its opt-in campaign, over 100,000 new supporters completed a new marketing permissions form with opt-in to mail tracking around 20 percent.**

**Cancer Research UK faced several challenges in its journey to become an opt-in charity:**

1) **Modelling.** Modelling the predicted impact was complex due to the number of variables.
2) **Complexity of touchpoints.** With over 150 different sign-up touchpoints, keeping track of the changes was complicated.
3) **Finding budget and resource.** The complexity of the project required intense resource and impacted other areas of the charity. Budget was needed for costs to deliver opt-in.
4) **Reporting.** The complex landscape required bespoke solutions at individual form level.
5) **Measuring impact.** It was challenging to understand what key metrics to measure.

**It is too early to measure the impact on direct marketing activity, but Cancer Research UK is confident it is the right move. It not only ensures their marketing is compliant with GDPR best practice, it will create deeper supporter trust, engagement and value in the long term.**

Source: Zoe Rowland, Head of Data Governance, Cancer Research UK

# CASE STUDY 2:
# HOME-SHOPPING BUSINESS

## A HOME-SHOPPING BUSINESS IS USING LEGITIMATE INTERESTS TO COMMUNICATE WITH CUSTOMERS UNDER THE GDPR

One of largest home-shopping organisations in the UK spends millions of pounds every year communicating directly with customers.

**ACROSS THE YEAR, CUSTOMERS RECEIVE 10–30 MAILINGS**

**The GDPR has become the biggest focus of the organisation. It started with a comprehensive mapping exercise to understand: what data it processes, what it is used for, where it is going and how it leaves the business – considering the legal basis for each.**

Following this, the organisation split its databases by recency, creating three bands based on the customers' last transaction dates. A separate assessment was conducted for each band to understand whether it was GDPR compliant and could continue to be mailed under legitimate interests. This led to the determination that mailing customers who have shopped with a brand in the top two recency bands would be in both the customers' and the brands' legitimate interests.

A further **10 per cent** of the organisation's communications are to cold prospects – it is uncertain as to whether legitimate interests are the right position to take with sourced data. Following a paper released by the Data Protection Network in July 2017, it **looks like the pooled data market** will be opting for **legitimate interests** as permission to continue to provide data to businesses to communicate with prospects. This is a position that the organisation plans to follow; however, it is aware that that the **guidelines around this remain sensitive and open to change.**

**THE ORGANISATION HOPES TO BE FULLY GDPR COMPLIANT BY 2018.**

> **How prepared are we? It changes daily, but it is likely that we will be there, or nearly there. What is clear is our intent and the processes we have put in place to get there.**

Source: Home-Shopping Business

# CASE STUDY 3:
# DEVELOPMENT CHARITY

## A DEVELOPMENT CHARITY IS RESEARCHING SUPPORTERS BEFORE IMPLEMENTING LEGITIMATE INTERESTS

**To ensure it would be in the best position to be GDPR compliant by May 2018, this development charity set up a working group spanning all departments and created GDPR "champions" responsible for pushing the GDPR agenda across their business area.**

**90–95%**
**RETENTION ACTIVITY**

With 90–95 per cent of the direct mail that it sends focusing on retention activity, it is vital that the charity ensures it is compliant, while at the same time maintaining the best interest of supporters and continuous income to help beneficiaries.

While not yet confirmed, the charity believes it is likely that it will use legitimate interests when communicating by mail. This position has been derived from aligning its vision with the requirements under the GDPR.

**As well as looking internally to support its decision to use legitimate interests when communicating by mail, the charity is carrying out an extensive research exercise with current donors, exploring how they want to be communicated to and what their expectations of the charity are when it comes to legitimate interests. The findings from the research will influence the charity's position.**

**Once the charity has finalised the changes in its privacy policy, it plans to communicate this to supporters in a bespoke mailing or, if the donor has opted in, email.**

**While the findings of the research have not yet been issued, the charity is confident that legitimate interests will be how it defines its position for communicating with supporters under the new GDPR requirements.**

Source: Development Charity

# HOW CAN WE HELP?

**Call on the power of Royal Mail MarketReach and Data Services to boost your marketing effectiveness.**

We're a dedicated team of specialists with a unique set of skills, tools and free services to help you make money. Our data planners and media specialists are on hand to enhance your marketing strategy through mail, so your campaigns get the best results possible.

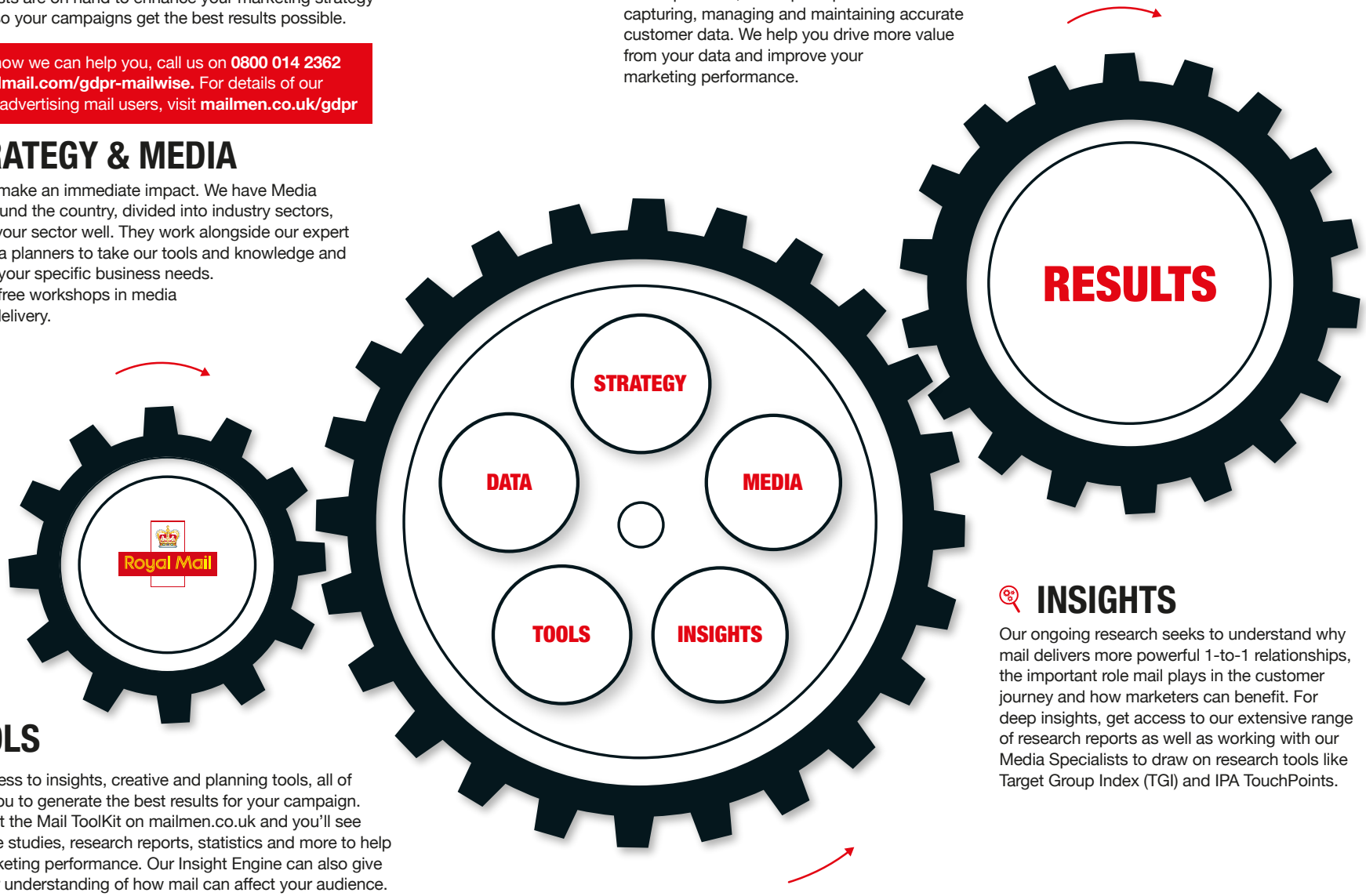
To discuss how we can help you, call us on **0800 014 2362** or visit **royalmail.com/gdpr-mailwise.** For details of our services for advertising mail users, visit **mailmen.co.uk/gdpr**

## STRATEGY & MEDIA

Our team can make an immediate impact. We have Media Specialists around the country, divided into industry sectors, so they know your sector well. They work alongside our expert media and data planners to take our tools and knowledge and apply them to your specific business needs.
We even offer free workshops in media planning and delivery.

## DATA SERVICES

Navigate the complexities of data and unlock its power for your business. Blending high-quality, industry-leading data with a depth of insight and experience, our experts provide services for capturing, managing and maintaining accurate customer data. We help you drive more value from your data and improve your marketing performance.




## TOOLS

We have access to insights, creative and planning tools, all of which help you to generate the best results for your campaign. Take a look at the Mail ToolKit on mailmen.co.uk and you'll see insights, case studies, research reports, statistics and more to help improve marketing performance. Our Insight Engine can also give you a greater understanding of how mail can affect your audience.

## INSIGHTS

Our ongoing research seeks to understand why mail delivers more powerful 1-to-1 relationships, the important role mail plays in the customer journey and how marketers can benefit. For deep insights, get access to our extensive range of research reports as well as working with our Media Specialists to draw on research tools like Target Group Index (TGI) and IPA TouchPoints.

# SOURCES OF FURTHER INFORMATION

**Information Commissioner's Office (ICO)**
www.ico.org.uk

**Direct Marketing Association (DMA)**
www.dma.org.uk

**Data Protection Network (DPN)**
www.dpnetwork.org.uk

**Federation of European Direct & Interactive Media (FEDMA)**
www.fedma.org

To discuss how we can help you, call us on **0800 014 2362** or visit **royalmail.com/gdpr-mailwise.** For details of our services for advertising mail users, visit **mailmen.co.uk/gdpr**

To discuss how we can help you, call us on **0800 014 2362** or visit **royalmail.com/gdpr-mailwise.** For details of our services for advertising mail users, visit **mailmen.co.uk/gdpr**