CIPR CHARTERED INSTITUTE OF PUBLIC RELATIONS

Introduction to the General Data Protection Regulation (GDPR)

#CIPR / @CIPR_UK

CPD 5

This guide is worth 5 CPD points

Contents

General Data Protection Regulation

1 Introduction

Your organisation's data processing activities represent a potential risk to the data subject and to the organisation itself.

You need to take steps to mitigate this risk, ensuring compliance with the General Data Protection Regulation (GDPR). The GDPR was approved by the EU Parliament on 14 April 2016. It will come into effect in the UK, imposing new duties, on 25 May 2018. For data processing to be lawful under GDPR, you must identify and document the legal basis your organisation relies on for each data processing activity before you process personal data and you should update your privacy notice to explain it. The six legal conditions are known as "Lawfulness of processing conditions":

(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

Where you rely on consent for processing, stricter standards under the GDPR mean the way in which you can gain consent from a data subject may be different.

The GDPR replaces the Data Protection Directive 95/46/EC and is intended to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organisations across the region approach data privacy. GDPR goes beyond the current requirements of the Data Protection Act 1998. It is quite possible that compliance with GDPR will result in changing the way you currently collect, process and store data. Following the introduction of the GDPR, your data processing activity must be communicated in a transparent manner – with particular attention paid to the question of consent.

Failure to comply with the GDPR creates a significant risk, through your use of technology in the processing of data and communication, in terms of business continuity. For example, a personal data breach could result in a "Stop Order", forcing a shut down of all data processing activity.

GDPR and Brexit

The Regulation will be enforced from 25 May 2018 before the UK leaves the European Union. The government's Statement of Intent on a new Data Protection Bill has underlined that the GDPR is here to stay even after Brexit. The full text of the UK's Data Protection Bill was published on 14 September 2018. It will repeal the Data Protection Act 1998 and implement the GDPR in full to prepare the UK for when it exits the EU. The Bill also deals with GDPR derogations and includes the introduction of new criminal offences. The Bill is currently going through the legislative process.

Leading compliance

"Data" is increasingly a subject of public interest and concern and the risk resulting from non-compliance with GDPR is considerable.

Complying with data regulation is a board level responsibility and the reputational impacts should also make it a key consideration for competent public relations professionals. Whether you process data for use in public relations activity or oversee a multi-disciplinary communication team, you should be aware of the compliance issues that arise from the GDPR and Privacy and Electronic Communications EC Regulations 2003, as well as the forthcoming ePrivacy Regulation and be in a position to advise your organisation about its responsibilities.

2 Key changes

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world. Although the key principles of data protection in the GDPR are consistent with the existing regime, the standards expected of data controllers and processors will be increased. There is now a new accountability requirement which means that organisations must not only comply with the requirements under the GDPR, but demonstrate compliance. Other significant changes include the expanded territorial reach of the GDPR, the stricter requirement for consent, the imposition of direct obligations on processors, not just controllers and the increased rights of data subjects.

Change in scope and penalties

GDPR applies to all organisations (controllers and processors) processing the personal data of EU resident data subjects, regardless of that organisation's location and whether the processing takes place in the EU or not. Whilst under existing data protection laws, a non-EU organisation will only be caught if it is established in the EU, the GDPR has a much wider reach. Non-EU organisations will be caught if:

- as a business, it offers goods or services (paid or free) to data subjects in the EU, or
- it monitors the behaviour of data subjects in the EU.

Non-EU organisations processing the data of EU citizens will also have to appoint a representative in the EU, subject to some limited exceptions.

Organisations in breach of the GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater) for the most serious infringements. It is important to note that these rules apply to both controllers and processors and 'clouds' will not be exempt from GDPR enforcement.

Consent
Consent provides one legal basis for processing personal data. Under the GDPR there is a higher standard for consent. Consent is defined as a "freely given, specific, informed and unambiguous indication of a data subject's wishes by which he or she, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Consent must be clear, easily distinguishable and provided in an intelligible and accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it. Organisations may need to look at their technology systems, eg: CRM, to assess whether they support them in demonstrating consent, as well as allowing the easy withdrawal of consent.

See Consent guidance.

Breach notification
Under the GDPR, there is a requirement to notify the supervisory authority of any data breach without undue delay and no later than 72 hours of becoming aware of the breach, where the data breach is likely to "result in a risk for the rights and freedoms of individuals". Data processors will also be required to notify their customers, the controllers, of all data breaches "without undue delay".

Controllers must also notify data subjects of a data breach involving their personal data unless the breach is unlikely to result in a high risk for the rights and freedoms of the data subjects, or appropriate technical and organisational measures were in place at the time of the breach eg. encryption. Where notifying data subjects individually would trigger disproportionate effort, it is also possible to issue a public information message or something similar, to notify data subjects.

Right of access (subject access requests)
The right of access is substantially similar under the GDPR as under the Data Protection Act 1998. Data subjects have the right to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed as well as access to the personal data and further supplementary information similar to the information that should be set out in a privacy notice including details as to the purpose for which the personal data is processed. The controller is required to provide the information free of charge except where the request is manifestly unfounded or excessive in which case a reasonable fee can be charged. Where the request is made electronically, the information should be provided in an electronic format. The GDPR also introduces a best practice recommendation that where possible, organisations should provide data subjects with remote access to a secure self-service system in order to be able to access the information.

Right to be forgotten
Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase their personal data, stop any sharing of their data, and potentially have third parties halt processing of the data too. This can happen where, for example, the data is no longer necessary for the original purposes for which it was processed or consent has been withdrawn. This part of GDPR requires controllers to compare the subjects' rights to "the public interest in the availability of the data". The right to be forgotten is not an absolute right and there are certain grounds on which the right can be refused including the right of freedom of expression and information or where the personal data is processed in the exercise or defence of legal claims.

Right to object to direct marketing
Data subjects have an absolute right to object to the processing of their personal data for direct marketing (including profiling) and there are no grounds on which the controller can refuse this.

Data Subject Rights
The full list of data subject rights, introduced or strengthened by the GDPR are as follows:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Visit the ICO website for more information.

Data portability
GDPR introduces the right for a data subject to receive their personal data, which they have previously provided in a "commonly used and machine readable format" and to have the right to transmit that data to another controller. This is not an absolute right and only applies in certain circumstances.

Privacy by design
Privacy by design requires data protection to be included in the designing of systems from the start and to be embedded in all data processing activities. The GDPR states: "The controller shall… implement appropriate technical and organisational measures… in an effective way… in order to meet the requirements of this Regulation and protect the rights of data subjects".

Only data absolutely necessary for the completion of its duties (data minimisation) can be processed and access to personal data is limited to those who carry out the processing.

Data protection officers
The requirement to appoint a DPO will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data, such as criminal convictions and offences. The DPO must be appointed on the basis of expert knowledge of data protection law. They can be an external service provider or in-house provided there are no conflicts with other tasks. They must report to the Board and be given sufficient resources to complete their task effectively.

How to prepare

Read the ICO's "12 Steps to take now"

Ask who is currently responsible for data protection in each context – i.e. where you are employed, or for your clients.

Understand whether, how and when to conduct information audits and Privacy Impact Assessments.

Review your data protection policies and procedures and ensure that these are compliant with the GDPR. Here are some questions to get you started:

1. Do they have clear, fair and transparent rules for obtaining data subjects' consent or set out another legal basis for processing? Is it as easy to withdraw consent as it is to give it?
2. Do they require the development of any new processes to include "privacy by design"?
3. Do they include a process for training all employees involved in collection and processing of data?

4. Do they include what to do in the event of a data breach?
5. Do they include a demonstrably clear idea of what harm breaches might do to data subjects such as customers/clients. i.e., financial fraud or identity theft.
6. Do they include a policy for destroying out-of-date data? Does your technology have this as an in-built option?
7. Do they include a mechanism for meeting a data subject's rights including a right of access and the right to be forgotten?
8. Do you need to appoint a DPO?

Review your client or agency and any (other) supplier contracts and ensure these contain adequate contractual protection to meet the needs of the GDPR.

3 Issues for public relations

Media Relations and the GDPR

The GDPR may affect how you manage media relations, particularly if you send unsolicited communications, such as press releases, to journalists.

Recording, storing or using contact information (which includes their work or corporate email addresses and social media accounts) means you are processing their data. Journalists have the same rights as any data subject under the GDPR.

In this guidance, we set out the general changes that you should make to comply with the GDPR. Whilst there is a difference between marketing communication and much of what may be communicated in public relations practice, the distinction may not be considered relevant.
We advise that you apply your GDPR preparation to your management of data relating to journalists.

To comply with the GDPR, you need to identify a legal basis before you can process personal data. These are often referred to as the "conditions for processing" under the DPA. It should be noted that consent is one of the six conditions that gives a legal basis for processing data, as set out in Article 6 (1).

The six legal conditions are known as "Lawfulness of processing conditions":

(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

It may be the case that public relations activity, where the processing of personal data belonging to a journalist is necessary, will be covered by the legal obligation condition (c) public interest (e) or the legitimate interests or the data controller condition (f). However, the CIPR strongly advises that you review the grounds for processing any personal data, including journalists. It may be that you need to seek consent when in doubt.

Practical tips

1. Review the legal grounds for processing personal data. Do you need to obtain consent from the journalist?
2. Review your media contacts. Do you and your organisation manage journalist's contact information in a GDPR-compliant way? (i.e. if you need consent, is it recorded? Does it meet the requirements of consent under the GDPR? Have you communicated privacy information to them?

See Consent guidance.

3. Review your communication around data processing for clarity and transparency – this includes when you communicate with journalists. Include your privacy notice as you would a boiler plate or notes to editors

See Privacy Notices guidance.

4. Where personal data is obtained directly from the journalist, privacy information should be communicated when the data is collected. For data not obtained directly from the journalist, this information should be communicated:

a. Within a reasonable period of having obtained the data (and in any event within one month)

b. If the data is used to communicate with the journalist, when the first communication takes place

c. If disclosure to another recipient is envisaged, before the data is disclosed

5. Check that your media database service providers and also any email newsletter service providers or marketing systems are compliant with the GDPR. Review your data management software and data processing and management practices to ensure compliance with the GDPR.
6. Ensure that unsolicited email contact is managed in terms of GDPR compliance as well as relevant marketing legislation including the Privacy and Electronic Communications Regulations 2003. Guidance on direct marketing is provided by the ICO and together with a direct marketing checklist.

For more information, visit the ICO website.

7. Under the GDPR there is no such thing as opt out consent and silence, inactivity, pre-ticked boxes won't suffice. Consent needs to be unambiguous which requires some clear affirmative action.
8. Check the compliance of any activities that borrow from or cross over into marketing and related legislation.
9. Review your crisis response communications planning – does it include data loss, failures in data security or other issues resulting in exposure of the data subject to greater risk?

4 Consent guidance

Consent provides one of the six lawful conditions for processing personal data.

There is a higher standard for consent under the GDPR. Consent is defined as any "freely given, specific, informed and unambiguous indication of a data subject's wishes by which he or she, by statement or clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Under the GDPR, consent must be:

- Unbundled
- Active
- Granular
- Named
- Easy to Withdraw

In terms of your administration, consent should be:

- Documented – keep records to demonstrate what the individual has consented to, including what they were told, and when and how they consented.
- Without 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, who may need to look for an alternative lawful basis such as legitimate interests, or necessary for the performance of a contract.

If you are considering how to ask for consent, you should read the guidance below:

Unbundled
What this means:

1. Consent must be separate from any other terms and conditions of service.
2. Consent may not be a precondition for the provision of the service unless the processing in question is necessary for the provision of the service.

Active
What this means:

1. The data subject must make a positive choice and take action to authorise processing of their data.
2. You may not offer a "pre-ticked" opt-in box for consent or opt out only consent.

Granular
What this means:

1. The data subject must consent separately to each type of data processing activity.
2. In practice this means each method of contacting them – email, SMS, phone or post, for example – and for each purpose of processing – account communications, marketing for example.

Named
What this means:

1. Clearly identify any organisation which will be relying on the consent to process the personal data.
2. This means clearly naming your organisation.
3. This means clearly identifying any third party organisation with whom you will share the data. The current ICO guidance on consent states that you need to name specific organisations rather than categories of recipients.

Easy to withdraw
What this means:

1. Data subjects can withdraw their consent at any time. It should be as easy to withdraw consent as it is to give consent.
2. You should have in place a mechanism that allows them to withdraw consent.
3. You should tell them clearly that they can withdraw consent at any time.
4. You should tell them clearly how they can withdraw consent. This should include the ability to withdraw consent via the same method it was originally given and be without detriment.

Consent form example

Box 1:

Terms and Conditions

To complete the purchase of [Product], please read and confirm your acceptance of our terms and conditions.

Click here to see our terms and conditions [LINK]

☐ I have read and accept the [company name here] terms and conditions.

These should generally cover other terms than data protection.

Box 2:

Can we contact you?

We would like to keep you in touch with what's happening at [company name here] and tell you about our events and special offers. To do this, we need to keep some personal data about you.

To find out what personal data we keep, how we process it and how we use it and to know more about your rights in terms of our use of your data, please read our Privacy Notice [LINK].

[Company name here] will not share your personal data with any third party organisations other than [names of those identified in your Privacy Notice or any regulator]. We would like, from time to time, to use your data to offer you access to [company name here] services, which may be relevant to you.

☐ I give consent for [company name here] to contact me about products and services

How may we contact you?

Please choose the methods by which you would prefer to receive information from [company name here]:

☐ Email

☐ Phone

☐ SMS

☐ Post

How to change your consent
You can alter the consent that you have provided at any time – and withdraw it at any time too.

Please click here to change your privacy preferences. [LINK]

Read the ICO's guidance on consent.

5 Privacy Notices guidance

How you should communicate privacy information will change under the GDPR.

Information about how and why you process someone's personal data informs their privacy and constitutes a privacy notice. Under the GDPR, information you provide to people about how you process their personal data must be:

- Concise, transparent and intelligible
- Easily accessible, written in clear and plain language (especially if addressed to a child)
- Provided free of charge

Currently, a privacy notice, shown when you collect personal data, has to give certain information, such as your identity and how you intend to use it.

Under the GDPR you will also need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data, amongst other things. The GDPR requires the information to be provided in concise, easy to understand and clear language.

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

What information should be included in a Privacy Notice under the GDPR?

- Identity and contact details of the data controller, its representative (if any) and the data protection officer (if any).
- The purpose of, and legal basis for, the processing of personal data.
- The legitimate interests of the controller or third party, where applicable.
- Categories of personal data to be collected (only where data is not obtained directly from the data subject).
- Any recipient or categories of recipients of the personal data (i.e. with whom data will be shared).
- Details of transfers to third country and safeguards.
- Retention period or criteria used to determine the retention period.
- The existence of each of the data subject's rights.
- The right (and details of how) to withdraw consent at any time, where relevant.
- The right to lodge a complaint with a supervisory authority. In the UK this is the ICO.
- The source the personal data originates from and whether it came from publicly accessible sources (only where data is not obtained directly from the data subject).
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data (only where the data is obtained directly from the data subject).
- The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.

As outlined in the ICO code of practice for privacy notices.

Writing a Privacy Notice

1. What – when writing a Privacy notice, you should consider:

- What information is being collected?
- Who is collecting it?
- How is it collected?
- Why is it being collected?
- How will it be used?
- Who will it be shared with?
- What will be the effect of this on the individuals concerned?
- Is the intended use likely to cause individuals to object or complain?

As a starting point it must include:

- Who you are
- What you are going to do with their information; and
- Who it will be shared with

The ICO states: "These are the basics upon which all privacy notices should be built. However, they can also tell people more than this and should do so where you think that not telling people will make your processing of that information unfair. This could be the case if an individual is unlikely to know that you use their information for a particular purpose or where the personal data has been collected by observation or inference from an individual's behaviour."

2. Where – A Privacy Notice is not necessarily a single document or page on your website. It encompasses all of the information you provide about the processing of personal data. The key principle is to ensure transparency about the processing you carry out. You can provide it in a range of ways and it is good practice to provide it via the same medium used to collect personal data.

a. It can be provided orally, in writing, through physical signage or electronically.

b. Where you use an online form to gather personal data, the privacy notice should be clearly accessible from within the form. Not provided separately via email or elsewhere on the website.

c. Consider this advice from the ICO:

"Take advantage of all of the technologies available when providing privacy notices. It may be valuable to consider these solutions after you have completed a privacy impact assessment. Examples of technological solutions include just-in-time, video, the functionality of devices and privacy dashboards. These can be seen as privacy-enhancing technologies, because they help to protect privacy and safeguard personal data. A blended approach, incorporating a variety of these techniques is likely to be most effective. Keep the individual as the focus when making decisions about the way to deliver privacy notices."

3. When should you actively communicate privacy information? If an individual would not reasonably expect you to process their data in the way you propose to, you need to actively provide privacy information, rather than simply making it available for them to look for themselves. For example, if you previously said you would not share their data with a third party, but now intend to do so you need to contact them with this information. Further, if you are collecting certain personal data and it is not reasonably obvious why you need that personal data, extra measures should be taken eg. collecting date of birth.

The need to actively provide privacy information is strongest where you are collecting sensitive information or the intended use or sharing of the information is likely to be unexpected or objectionable. It may also arise where providing personal data or not providing it, could have detrimental effect on the data subject. To find out what may be expected or objectionable, if you are in doubt, consider how you can research your intended audience.

Tips for writing and communicating privacy

1. Be Competent and Professional

- Be aware of the ICO's guidance and the general context and principles of data protection and the GDPR
- Be aware of any sector specific regulations or conventions on the use of data and privacy
- Use research to understand your audience if necessary
- Act with integrity and refer to the CIPR Code of Conduct
- Ensure you take vulnerable people, people for whom English is not their first language and people who may not have access to a range of technology into account when communicating privacy

2. Use Plain English

- Write in a clear and straightforward style
- Use a style your audience will find easy to understand
- Do not assume your audience has the same level of understanding
- Do not use jargon or legalistic language
- Be transparent

3. Consider the user experience when designing privacy communication

For example:

- "layered" information can include clear headlines, collapsible information and links.
- "Just in time" information, which appears on the screen when a data subject is about to share personal data.

Privacy Statement example

Last updated: [date here] – what's new? ([Link to updates]

[Company name here] is committed to protecting your privacy and complies with the principles of the relevant data protection regulations.

This privacy policy explains how and why we collect your personal data and how it is used.

About [company name here] and our Data contacts

- Personal Data we collect
- How we use personal data
- Who we share personal data with and why
- How you can access and update your information
- Your data and your rights
- How you can withdraw consent for us to use your data
- Our Security and your data
- Profiling
- Use of Cookies
- Links to websites
- 16 and under
- Transferring information outside Europe
- Reviewing the Policy

The above are suggested headings for your Privacy Statement.

When should privacy information be communicated?
Where personal data is obtained directly from the data subject, this information should be communicated when the data is collected.

For data not obtained directly from the data subject, this information should be communicated:
- Within a reasonable period of having obtained the data (and in any event within one month)
- If it is used to communicate with the data subject, when the first communication takes place
- If disclosure to another recipient is envisaged, before the data is disclosed

Read The ICO code of practice on privacy.

Other Resources
CIPR Members have access to a webinar on the GDPR *here.*

Share your feedback
If you would like to share your feedback on this guide or there is further information you'd like us to include, *please email philm@cipr.co.uk*