






The GDPR Survival Guide

insightdata
business is better with insight



The GDPR Survival Guide

	Introduction	1		Legal Grounds of Processing	8
	The Principles of the GDPR	2		Consent vs Legitimate Interest	11
	Individuals Rights	4		Demonstrating Accountability	12
	Security	5		PECR	14
	Preparation	6		Glossary	15



What is the survival guide?

Insight Data Ltd provide this GDPR Survival Guide out of goodwill and with the intention to help organisations with compliance. However, please be aware that the contents of this paper do not constitute legal advice and should not be relied on as such.

Introduction to the GDPR

The GDPR

On the 25th of May 2018 the General Data Protection Regulation sweeps across the UK, changing the way privacy and data protection is handled. This GDPR survival kit will provide you, in marketing terms, with advice and tools on how to approach your processes regarding data protection. Understanding all the GDPR terminology, the rights of data subjects, the 6 legal grounds of processing, privacy by design, whether you need a DPO (Data Protection Officer) and much more will help tackle the myths of the GDPR.

What is the The GDPR?

The Data Protection Act 1998 has found itself falling behind the rapid technological evolution of the past 20 years. Development of a new regulation by the EU has been well overdue. The GDPR is designed to synchronise all data laws across the EU and aims to protect and empower EU citizens, reshaping the way all organisations approach data privacy for the better.

The GDPR is agreed law across the European Union and a deadline of 25th of May 2018 was agreed for all members to have the regulation implemented. Although the United Kingdom is due to leave the EU following the 2016 referendum, the GDPR will still be introduced in its own form, known as "The Data Protection Act"; which will be designed to mirror the GDPR. This has been confirmed by the current UK government.

The GDPR applies to any information relating to an identified or identifiable natural person either directly or indirectly. From an organisational point of view, this may include any data held on employees, customers, ex-customers, job applicants, suppliers and prospects. It is almost certain that your organisation will have to acknowledge the GDPR and you may have to make some changes.



The Principles of the GDPR

What are the principles?

Under the Data Protection Act 1998, 8 key principles were set out for processors and controllers to abide by. The GDPR has adopted a similar stance outlining 6 principles under Article 5 of the GDPR. These are essentially the 6 commandments of the GDPR. Article 5 (2) states- “the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

Personal data shall be:

- a** Processed lawfully, fairly and in a transparent manner in relation to individuals;
- 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 not be considered to be incompatible with the initial purposes;
- c** Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d** Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
- e** Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- f** Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

So what do the principles mean to you?



In brief, this means that the personal data you hold and process must have been collected from individuals in a fair and open way. Do the data subjects know what you are doing with their data? If that is not clear, you may not be acting in a fair and transparent way.

Is the personal data you hold relevant for the purpose you intend to use it? If you are marketing windows to a cleaning company is it right that you carry on holding and processing that information? If you hold information on the data subject's religious beliefs, is that necessary for promoting conservatory roofs too?

Is the information held about the data subjects accurate and up-to-date? Causing harm or distress to data subjects can lead to investigations taking place in your organisation. Sending the wrong information to the wrong person has the potential to cause distress or harm. Taking reasonable steps to collect/acquire up to

date data is vital.

How long are you holding that PII (Personal Identifiable Information) for? This relates closely to the previous point. Justifying how long you hold that PII and how it is kept accurate is necessary to comply with the GDPR. Would you like a company to be holding old information about you from 2-3 years ago?

Do you have the right protocols in place to ensure the data subject's information held is protected from accidental loss, destruction or damage? Internal company policies on how data is transferred should be considered.

Is the information held safely stored and secured away from any threats? For example, if your staff have laptops, is the information fully secured if the laptop goes missing? Having appropriate measures in place to ensure the security of the personal data held is significant to complying with the GDPR.

Individuals' Rights

Individuals' Rights have been subject to abuse in previous years, something the GDPR is designed to eradicate. Individuals' Rights of the previous Data Protection Act 1998 are still in principle in the GDPR; However, they have now been refreshed and extended. In addition to revamping previous rights, the GDPR has created more clear and concise rights, meaning there are now 8 rights in comparison to the 6 provided by the Data Protection Act 1998.

What are the GDPR Individuals' Rights?

- 1. The Right to be Informed** - Individuals have the right to be informed as to why, how, and when their information will be processed, and what information is being used.
- 2. The Right of Access** - The GDPR explains in clear language that data subjects have the right to access the data held about themselves.
- 3. The Right to Rectification** - Individuals have the right to rectify their personal data if it can be proved that the data held is either incomplete or inaccurate.
- 4. The Right to Erasure** - The right to erasure can also be known as 'the right to be forgotten'. Individuals can request that the personal information held about themselves can be removed.
- 5. The Right to Restrict Processing** - Individuals can restrict their personal data by requesting it to be blocked or suppressed from processing.
- 6. The Right to Data Portability** - The right to data portability gives individuals the right to reuse their own personal data across different services.
- 7. The Right to Object** - Individuals have the right to object about how their data is being processed.
- 8. The Rights related to automated decision making including profiling**- Individuals can access any of their rights related to any form of automated decision making relating to them as a natural person.

The Data Protection Act 1998 Individual Rights-

1. A right of access to a copy of the information comprising their personal data;
2. A right to object to processing that is likely to cause or is causing damage or distress;
3. A right to prevent processing for direct marketing;
4. A right to object to decisions being taken by automated means;
5. A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed;
6. A right to claim compensation for damages caused by a breach of the Act.

Security

Section 2, article 32, 33 and 34 of the GDPR go on to give the rulings around appropriate security measures required to comply with the GDPR. Security has been highlighted as a key part of the GDPR and should be taken very seriously. Article 32 (2) states “In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.”

Article 32 (1) explains that “the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security relevant to the risk”. Appropriate measures could be;

- (a) the pseudonymisation and encryption of personal data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability of, and access to personal data in a timely manner in the event of a physical or technical incident;
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.



Where do I report a breach?

Accessing the ICO’s website under the ‘report a breach’ section will give you relevant information required to correctly report the breach.

<https://ico.org.uk/for-organisations/report-a-breach/>

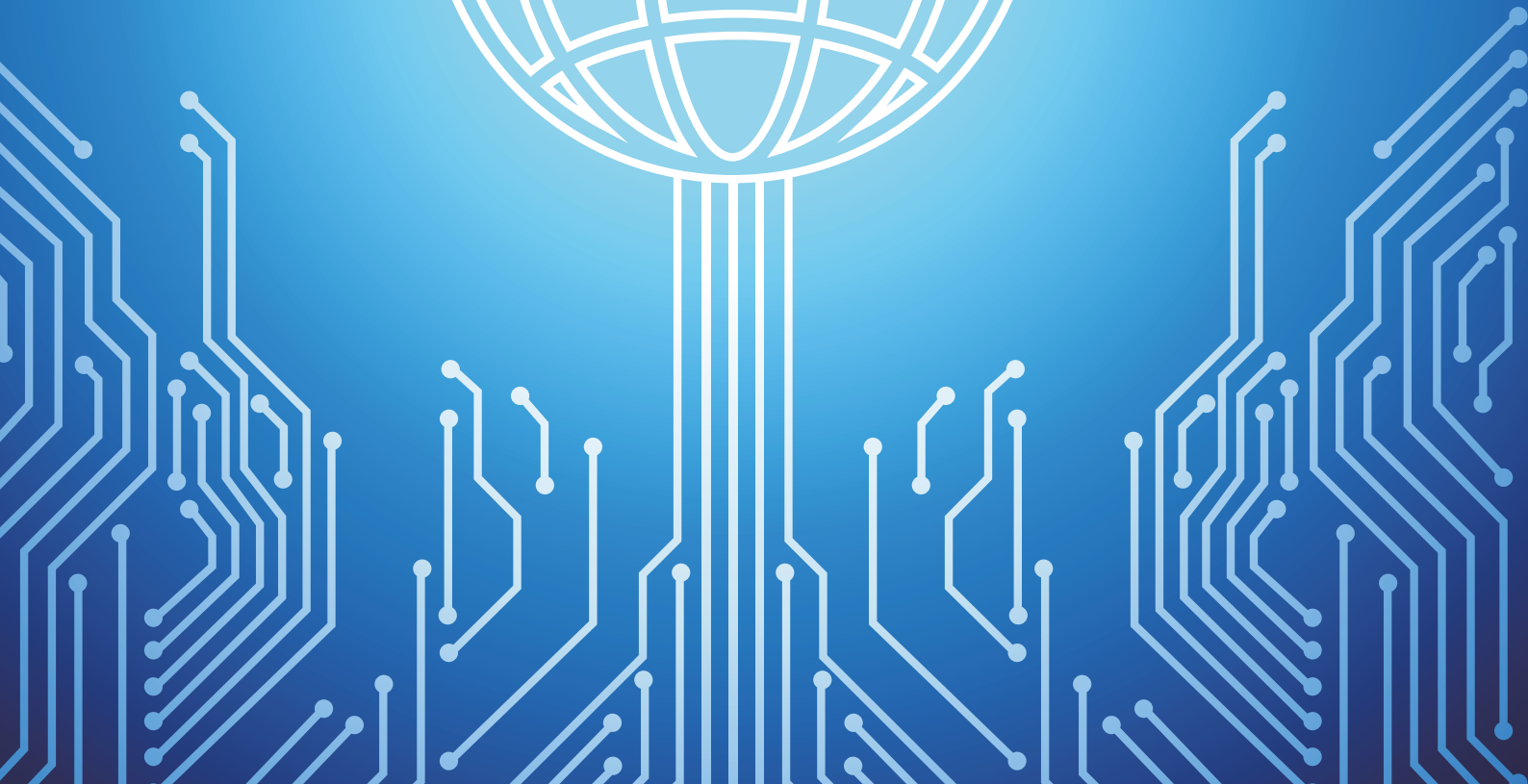
What is a data breach and what should I do if one occurs?

A data breach could be loss of data, alteration of the data, wrong access to the data or unauthorised disclosure of the personal data held. If the breach is likely to affect individuals’ rights and freedoms, you must act quickly.

The GDPR requires you to report a data breach to the relevant supervisory authority, in the UK, this would be the Information Commissioner’s Office (ICO). You have 72 hours to make the ICO aware of a data breach where practical. In some cases, you may need to inform the individuals who have been breached of what has happened, especially if their rights and freedoms are under threat.

Recital 85 of the GDPR states “A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.”

**“BY FAILING TO PREPARE,
YOU ARE PREPARING
TO FAIL.”**



Preparation

Significant preparation is required to comply with the regulation. Organisations need to strategically plan for 'gold standard' compliance.

Before you can start absorbing the 99 articles set out in the GDPR, it is important to understand what data you currently hold, where that data was sourced and with whom that data is shared.

Do I need a DPO?

DPO- Data Protection Officer

Section 4, Article 37 of the GDPR states;

'The controller and the processor shall designate a Data Protection Officer in any case where:

- (a) The processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- (b) The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- (c) The core activities of the controller or the processor consist of processing on a large scale, special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.'

If a DPO is required: do you know where to find one and what will their duties be?

Article 39 of the GDPR outlines 5 key tasks any DPO should undertake;

to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

to monitor compliance with the Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

to provide advice where requested as regards to the data protection impact assessment and monitor its performance pursuant to Article 35;

to cooperate with the supervisory authority;

to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.



REMEMBER

There is no such thing as a 'GDPR certified expert' as there is no accreditation body providing official qualifications regarding the GDPR.

The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Deciding Your Legal Ground of Processing Data

What is a legal ground of processing?

The GDPR states you must process all personal data lawfully, fairly and in a transparent way. To process data, you must use 1 of the 6 legal grounds provided under Article 6 of the GDPR. To comply with Article 5 (2) (Accountability) you will have to prove the reasoning behind why and how you use the lawful ground(s). The legal ground chosen should reflect your organisational use of personal data and will always be in favour of the individual's rights and freedoms. It is important that there is no hierarchy within the legal grounds of processing. None of the grounds are stronger than any of the other.



Legal Ground of Processing Data - What the GDPR says?



Consent

Consent - "The data subject has given consent to the processing of his or her personal data for one or more specific purposes;". Consent then goes on to be defined in Article 4(11) as follows: 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;"

Contract - "Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;". Article 6(1)(b), Contract is a legal ground for processing in order to fulfil contractual obligations or because the data subject has asked you to do something which involves processing their data before entering a contract.



Contract



Legal Obligation

Legal Obligation - "Processing is necessary for compliance with a legal obligation to which the controller is subject;" Legal Obligation is a lawful basis to use when processing personal data to abide with common law or statutory obligation.

Vital Interest - "Processing is necessary in order to protect the vital interests of the data subject;" Vital Interest is in place as a lawful basis if processing data is required to protect someone's life.



Vital Interest



Public Interest

Public Interest - "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;" Public Interest means data may be processed on the basis that such processing is necessary for the performance of tasks carried out by a public authority or a private authority acting in the interests of the public.

Legitimate Interest - "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". Legitimate Interest is the flexible lawful basis for processing personal data.



Legitimate Interest



Deciding Your Legal Ground of Processing - Data vs Simplified



Consent

Consent:

Very clear rulings are set out in the GDPR regarding consent. The text can be read as essentially saying that consent requires a positive opt-in so the previous way of some organisations using pre-ticked boxes, or any other pre-meditated method of consent, will no longer be valid. It is worth noting that bundling a consent statement within your Terms and Conditions will not be valid.



Contract

Contract:

Contract can be used in situations where, for example, a quote has been requested or there is a need to get in contact regarding a warranty. However, using the contract to identify the individual's interests and preferences based on purchases made to send targeted advertising is not classed as necessary and therefore should not be relied on as a valid ground of processing in that context.



Legal Obligation

Legal Obligation:

Legal Obligation has had very little change from the Data Protection Act of 1998. If you are processing data using this ground, it's worth reviewing current documentation to ensure justifying the decision to help with accountability. Legal Obligation does not coincide with contractual obligations. The processing of personal data must be necessary for processing using Legal Obligation.



Vital Interest

Vital Interests:

As with Legal Obligation there has been very little change in comparison to the Data Protection Act of 1998 other than anyone's vital interests can now provide a basis for processing compared to the previous ruling of only those data subjects themselves. Like with Legal Obligation, it is recommended that if you used this ground previously you revisit any documentation made to align with accountability and that the processing must be necessary to undertake Vital Interests.



Public Interest

Public Interest:

Public Interest can include processing data on the occasion of an exercise of a function conferred on a person by an enactment or the exercise of a function of the Crown, a Minister of the Crown or a government department.



Legitimate Interest

Legitimate Interest:

To use Legitimate Interest as a legal ground of processing there are three key elements to consider:

- 1) Can you identify a Legitimate Interest?
 - 2) Can you demonstrate that processing the personal data is necessary to achieve the Legitimate Interest?
 - 3) Can you demonstrate you have balanced the Legitimate Interest against the rights and freedoms of the individual's?
- Legitimate Interest will be likely used when the data subject can reasonably expect their data to be processed and it will have minimal impact on their privacy.



All 6 legal ground
of processing
hold equal value
in the GDPR

Consent

VS

Legitimate Interest

In nearly all cases regarding direct marketing, the two legal grounds will be either Consent or Legitimate Interest. Below we have drawn up the key points to consider for both Consent and Legitimate Interest.

Consent

- ✔ Consent must be clear and unambiguous when offered to data subjects.
- ✔ Consent must be a real choice to the individuals. It cannot be forced or hidden. Remember the data subject should have control over what they have consented into.
- ✔ Positive opt-ins are required to meet the standard of consent. Previously, consent could be gained under “soft opt-in” (e.g. pre-ticked “consent” boxes). These methods will no longer be valid to prove compliance.
- ✔ Consent must be specific. An unclear or vague consent statement is not sufficient.
- ✔ Document when consent was taken, how it was obtained, who it was obtained by and what the consent is for.
- ✔ It must be clear and easy for data subjects to withdraw their consent at any time.
- ✔ Name any organisations or third-party controllers to whom the personal information will be passed. Consent must be clear so grouping companies together under consent may not be enough to prove legitimacy.

Legitimate Interest

- ✔ Consider carefully whether Legitimate Interest is the most appropriate ground to use. Are your Legitimate Interests at the cost of the fundamental rights and freedoms of the data subject?
- ✔ Conduct an LIA (Legitimate Interest Assessment) to demonstrate accountability in accordance with Article 5(2). A review should be conducted at any point that the circumstances change.
- ✔ Would the data subject expect their information to be processed by you, in the manner intended?
- ✔ Are there appropriate safeguards in place for data breaches?
- ✔ Are the data subjects informed clearly that their data is being processed under the Legitimate Interest grounds?
- ✔ Do the data subjects have easy access to opt-out at any point?
- ✔ Are the details of your Legitimate Interests included in your privacy policy?



Demonstrating Accountability

Why is accountability important?

The GDPR promotes a transparent view of data protection. This means that demonstrating accountability is paramount to compliance. Article 5(2) of the GDPR requires you to demonstrate compliance.

Some examples of how to demonstrate compliance have already been mentioned within this guide. The following is a list of some additional recommendations:



**GUILTY UNTIL
PROVEN INNOCENT**

Article 5(2)- "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

Demonstrating compliance

Below are some suggested documents to produce and things to consider regarding your journey to demonstrating compliance.

1. Assessment of current privacy practices

Identify what you are currently doing, whether it is inline with the GDPR or not? Document what you have investigated, for example what data you hold and where it was sourced. Look at your current procedures for dealing with erasures.

2. Conduct a DPIA

As stated earlier within the guide, a DPIA will assess the risk and problems of what you are currently doing. By highlighting the risks, you will be able to manage how best to handle any situations.

3. Create a data privacy structure within your organisation

Implementing Privacy by Design as a principle within your organisation will help towards compliance. Having an individual or team in charge of the implementation is suggested.

4. Reviewing all notices

Are all your privacy policies and cookie policies all up to date and written in a clear and transparent manner?

5. Consider certain measures to meet the principles of the GDPR

Data minimisation, pseudonymisation, transparency, reviewing how individuals can monitor processing, improving security are some measures which could be undertaken to meet the principles of the GDPR.

Article 24 of the GDPR- Responsibility of the Controller

“Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation. Those measures shall be reviewed and updated where necessary.”

Article 30 of the GDPR- Records of processing activities

“Each controller and, where applicable, the controller’s representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

- a) the name and contact details of the controller and, where applicable, the joint controller, the controller’s representative and the data protection officer;
- b) the purposes of the processing;
- c) a description of the categories of data subjects and of the categories of personal data;
- d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries (country outside the EU) or international organisations;
- e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- f) where possible, the envisaged time limits for erasure of the different categories of data;
- g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).”

Having a clear and transparent Privacy Policy

The GDPR promotes transparency and fairness throughout the text. In fact, the first principle under Article 5 of the GDPR states data should be processed ‘lawfully, fairly and in a transparent manner’. It is strongly recommended that your privacy policy should be reviewed to meet the accountability statement in Article 5. It is suggested that your privacy policy should at least;

- Identify who the controller is
- Identify why you are processing the data and why it is fair
- Explain who has access to the data
- Outline how the data was collected
- Identify how the data will be used
- Outline what type of information you hold. Is it sensitive?
- Inform the data subject on how long their data is held for
- Record if your data is shared with anyone else, and who?
- Outline the individuals rights (Article 15-22)
- Indicate who the data subject needs to contact if they object (internally to your organisation and the ICO)

Any information further to the points mentioned above which has an impact on the data subject’s rights and freedoms, should be explained in the Privacy Policy. Remember, your Privacy Policy should be written in clear English and if you process data on children, the policy must be in a format easy for children to understand as well as adults.

PECR



What is PECR?

Privacy and Electronic Communication Regulations, more commonly known as PECR, specifically govern any electronic communication. This could be marketing calls, emails, texts, faxes and cookies. PECR is a separate regulation from the GDPR, however PECR is soon to be replaced by the E-Privacy Directive.

PECR refers to any direct marketing sent via electronic means. Direct marketing is defined in section 11(3) of the Data Protection Act 1998 as: “the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals”.

It is important to remember that most of the rules in PECR apply to unsolicited marketing messages. That could be a message sent which has not been specifically requested. However, if someone ‘opts in’ to receive marketing from you, this does not count as solicited marketing. Although the subject has agreed to future messages, it is not the same as someone specifically contacting you to ask for a specific piece of information. You can still send unsolicited marketing messages if you comply with PECR.

The PECR rules in brief



Telephone Rules

Regulation 21 of PECR states you cannot make unsolicited live calls to anyone registered with the TPS or CTPS unless they are an existing customer or have consented to you calling them. Anyone who tells you they no longer want to receive your calls must not be contacted.



Email Rules

Regulation 22 of PECR states you cannot send electronic mail to individuals unless they have specifically consented to receive information, or they are an existing customer who bought (or negotiated to buy) a similar product or service from you in the past. It is important to note, you can email any limited, LLP or government body if you offer an opt out option when contacting. Sole traders and some partnerships are treated as individuals.



Fax Rules

Regulation 20 of PECR states you cannot send marketing via fax if the number is registered with FPS, the individual has told you they don't want to receive any marketing, or you haven't gained specific consent to do so.



Cookie Rules

Regulation 6 of PECR states that you should inform individuals that the cookies are there, what they are doing and why they are there. You will need consent to store a cookie on their device.

PECR changing to the E-Privacy Regulation

It is worth noting PECR is due to be replaced by the E-Privacy Regulation currently being lobbied within the EU. This is effectively to work alongside the GDPR. There may be changes to the text between now and its estimated date of completion around May 2019.

GDPR Glossary

Word/Phrase	Official Definition	Easy to Understand Definition
The GDPR	The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). The GDPR begins officially on the 25th of May 2018.	<p>A set of rules/guidelines produced within the European Union outlining new rights for individuals regarding their personal data being used.</p> <p>The GDPR will then be introduced into each country's legislation turning it into law retrospectively.</p>
The DPA 1998	The Data Protection Act 1998 (DPA 1998) is an act of the United Kingdom (UK) Parliament defining the ways in which information about living people may be legally used and handled. The main intent is to protect individuals against misuse or abuse of information about them.	The current laws on data protection introduced in 1998 by the UK government outlining how personal information can be used by organisations or individuals.
The DPA 2018	The Data Protection Act (DPA) will be the new act of the United Kingdom (UK) Parliament aligning with the GDPR, giving information about how personal data can be legally used and handled.	The Data Protection Act, due to come into force on the 25th of May 2018, will be the updated version of the current DPA 1998. This DPA will mirror regulations set out in the GDPR ensuring the UK's ability to process, control and transfer data abiding by the EU rules.
Data Controller	The Data Controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.	The Data Controller is someone who decides what happens to the individual's data held.
Data Processor	In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.	The Data Processor performs the request made by the Data Controller.

Word/Phrase	Official Definition	Easy to Understand Definition
Processing	In relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.	Processing can include, <ul style="list-style-type: none"> • Organisation, adaptation or alteration of the information or data. • Retrieval, consultation or use of the information or data, • Disclosure of the information or data by transmission. • Dissemination or otherwise making available, • Alignment, combination, blocking, erasure or destruction of the information or data.
Data Subject	The Data Subject is a living individual to whom personal data relates.	A person whose data can be related back to them.
Privacy by Design	Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. Unfortunately, these issues are often bolted on as an after-thought or ignored altogether.	Privacy by design means having the mindset that privacy and data compliance is at the forefront of all aspects of data controlling or handling from the outset, rather than introducing the protocols further down the line.
Personal Data	Any information relating to an identified / identifiable individual, whether it relates to his or her private, professional, or public life.	Any data which reveals the identity of the individual.
DPO	A data protection officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with the GDPR requirements.	Someone who is responsible for your organisation's data protection, the GDPR compliance and ensuring the individuals rights are met during the controlling and processing period of their data being stored.
Profiling	Any form of automated processing of personal data using it to evaluate, analyse or predict certain personal aspects of a natural person.	Processing the data in an automated way which you can then use to evaluate, analyse or predict traits of a natural person. Examples of profiling explicitly listed in the text of the GDPR are: performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Pseudonymisation	The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.	A procedure by which the most identifiable fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. There can be a single pseudonym for a collection of replaced fields or a pseudonym per replaced field.

Word/Phrase	Official Definition	Easy to Understand Definition
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 individual giving a clear indication that they are happy for their data to be used in the way expressed at the point of collection.
Legitimate Interest	<p>Legitimate Interest is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate.</p> <p>It is likely to be most appropriate where you use people's data in ways they would reasonably expect, and which have a minimal privacy impact, or where there is a compelling justification for the processing.</p>	The lawful basis for processing based on identifying the interests and rights of the data subject in question. Deciding whether the marketing material you are sending is the most appropriate basis for ensuring that the processing is low risk and not likely to cause the individual harm.
The ICO	The Information Commissioner's Office (ICO; stylised as ico.) in the United Kingdom, is a non-departmental public body which reports directly to Parliament and is sponsored by the Department for Digital, Culture, Media and Sport (DCMS).	The authority who polices, advises and assists with any data related issues.
Article 29 Working Party	The Article 29 Working Party (referred to as "WP29") is made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. The composition and purpose of WP29 was set out in Article 29 of the Data Protection Directive, and it was launched in 1996. WP29's mission is to provide expert advice to the EU Member States regarding data protection and promote the consistent application of the Data Protection Directive.	A group of experts in data protection from EU member states who provide advice for law makers regarding the GDPR.
PECR	The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act. They give people specific privacy rights in relation to electronic communications.	Also derived from European law, PECR or 'the e-privacy directive' complements the existing data protection regime but is more specific on the rights of individuals regarding electronic communications. This can include email, SMS messaging, fax, telephone marketing and cookies.

insightdata
business is better with insight



Unit 502, Worle Park Way, Weston-super-Mare, BS22 6WA
T: 01934 808 293 | **F:** 01934 625 027 | **E:** hello@insightdata.co.uk
twitter.com/insightdata | insightindex.co.uk/in/insight

www.insightdata.co.uk