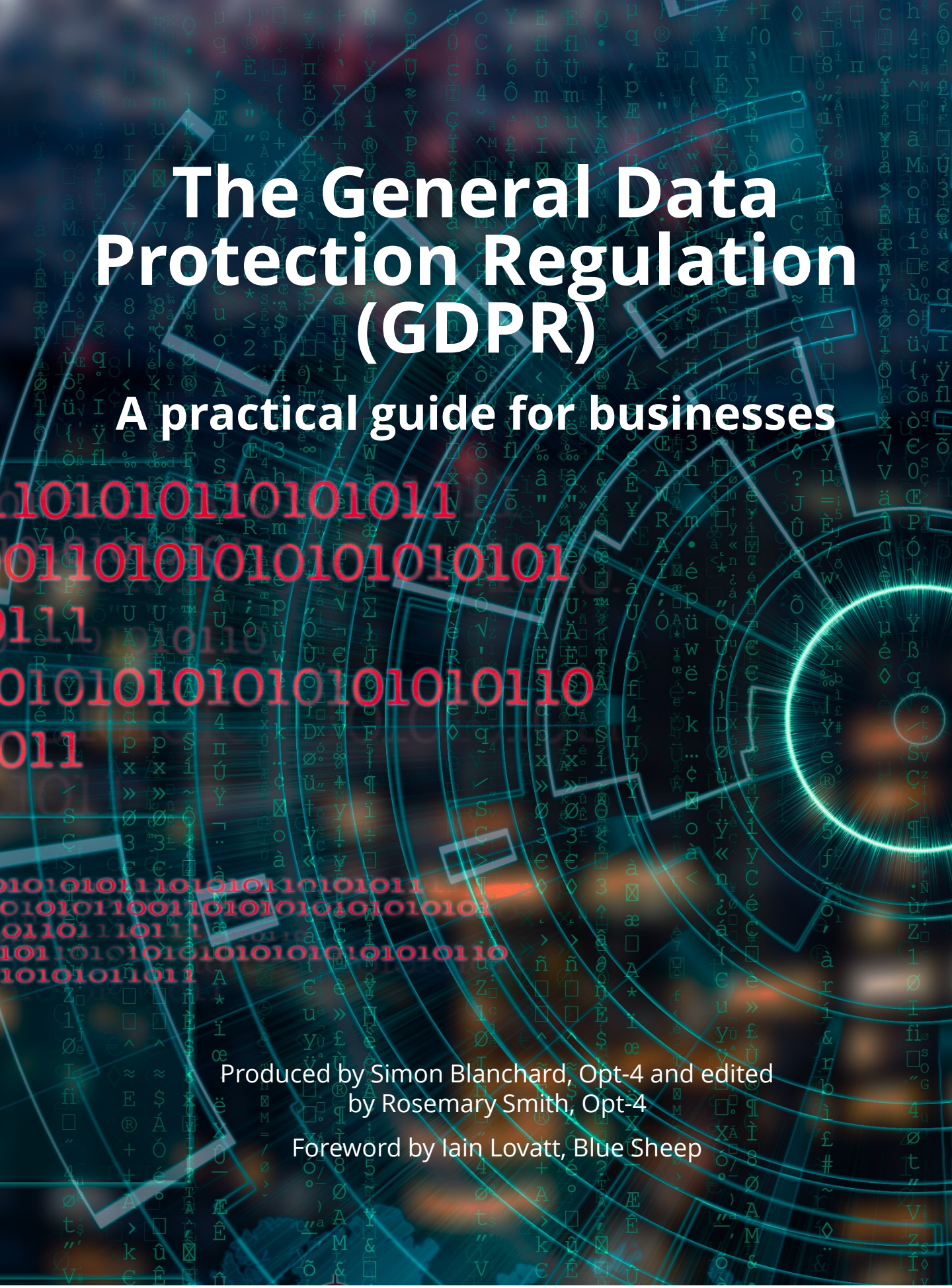


The General Data Protection Regulation (GDPR)

A practical guide for businesses

Produced by Simon Blanchard, Opt-4 and edited by Rosemary Smith, Opt-4

Foreword by Iain Lovatt, Blue Sheep

Blue Sheep®

Copyright Opt-4 & Blue Sheep, August, 2016

OPT-4

Foreword

The many implications of Britain's decision to leave the European Union are still years away. However, one thing that will not change is a revision of the country's current data protection laws.

In October 2016, the UK Government confirmed that it will be adopting the General Data Protection Regulation (GDPR), at the very least until 2019 when the country completes its exit from the EU.

Beyond that, if the UK wishes to continue trading with the EU (and it will), then it will still need appropriately 'adequate' data protection laws. They perhaps may not be identical to GDPR, but broadly similar enough to justify the need for long-term compliance.

This means there is no more time for indecisiveness. Businesses need to understand the regulations, the changes and the impact now.

Whether your organisation is based in or outside the EU, if your business handles the customer data of any EU citizen then your current practices for collecting, using and sharing data will need to be assessed.

In order to comply with GDPR, marketers will need to maintain cleaner and more accurate databases, provide more transparency with how data is handled and put in more security measures to prevent data breaches.

This extensive guide has been created by our friends at Opt-4 to help you better understand the new approaches to customer profiling, processing and consent, and a landscape where marketers will need to work harder to obtain consent for using someone's data.

Still, a fresh look at the relationship you have with your customers and an opportunity to build a new foundation of trust and openness will positively affect the customer experience and encourage loyalty – no bad thing for any brand. It is almost certainly more favourable than a non-compliance fine that runs into the tens of millions of Euros!

At BlueVenn, we are well placed to help you better manage your customer data and in conjunction with Opt-4 can help ensure it is accurate, compliant and conforms to all the requirements for permission.

Iain Lovatt, Chairman, Blue Sheep

www.bluesheep.com

Contents

Introduction

The General Data Protection Regulation (GDPR) is a new piece legislation approved by EU Member States which is designed to protect the data and fundamental privacy rights of all EU citizens.

The UK's Data Protection Act 1998 was derived from EU Directive 95/46/EC which dates back to 1995. Other EU Member States also have their own data protection legislation derived from that Directive. When the current Directive was written, the internet and email were still very much in their infancy and social media had not yet been invented. The world of data has exploded since then and the European Commission decided that new legislation was needed to protect individuals from misuse of their data in the modern, digital age.

As the name suggests, GDPR is a Regulation not a Directive, which means it will go into force across all EU Member States without any changes to the text. The final version of the text has now been agreed and so GDPR will come into force on 25th May 2018.

It has been now been confirmed that the UK will adopt GDPR while the country is a member of the EU. After that, as UK citizens will no longer be EU citizens, then it is expected that the country will have broadly similar data protection laws, to ensure "adequacy" with the GDPR so the UK will be able to continue trade with EU and maintain personal data protection rights.

Therefore, the principles and definitions laid down in the GDPR will be applicable to all UK organisations. Any businesses which market to EU consumers will have to abide by GDPR anyway.

Introduction

GDPR consists of 99 Articles, plus 173 Recitals, which provide explanatory text to aid interpretation of the Articles.

Even with these Recitals, there are some topics which require further clarification to explain how GDPR should be interpreted by organisations.

At the time of writing (August 2016) there has been no official guidance from the Supervisory Authorities (i.e. the data protection regulators in each State).

It is therefore inevitable that interpretations of the Articles and Recitals will change as and when guidance is produced.

Areas which are subject to such interpretation are noted in this White Paper.

Article and Recital extracts from the GDPR text are highlighted in blue.

What is 'Directivisation'?

The term 'Directivisation' means that certain requirements of the GDPR may be derogated to local Member State law.

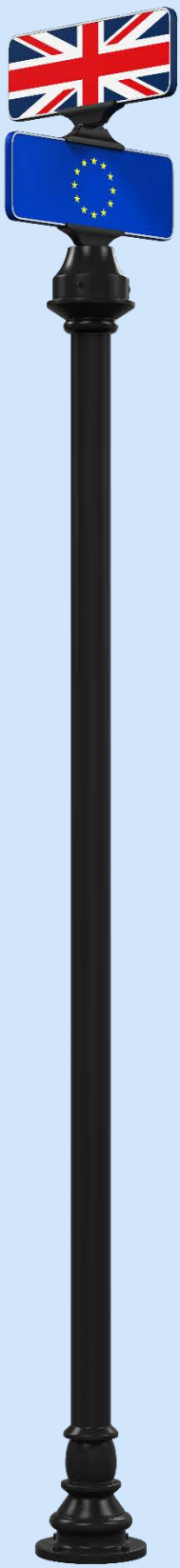
For example, at what age an individual would be classed as a child or an adult, or when a Data Protection Officer needs to be appointed.

There are more than 50 instances of potential derogations to local Member State law in the GDPR.

There are also instances where guidance can be provided by the newly created European Data Protection Board, or by local regulators.

In practice, this means the Regulation will not create a completely uniform regime throughout Europe.

The Global Scope of GDPR



GDPR will apply to all organisations which have EU “establishments”, where personal data are processed “in the context of the activities” of an establishment. This applies irrespective of whether the actual data processing takes place in the EU or not.

Non-EU organisations will be subject to the GDPR where they process personal data about EU citizens in connection with:

- The “offering of goods or services” (payment is not required); or
- “Monitoring” their behaviour within the EU.

The impact of this for companies which market internationally is that they will have to apply GDPR rules to the processing of personal data of individuals within the EU even if the processing takes place elsewhere.

Practically, it may be simpler to apply GDPR rules to all data processing.

Other Regulations & Directives

When GDPR comes into force it will not stand alone as the only regulation affecting data-driven communications to individuals in the EU. A new ePrivacy Directive (replacing the existing one from 2002) is currently under consultation, which will set additional requirements for organisations.

The 2002 Directive led to the UK’s current Privacy and Electronic Communications (EC Directive) Regulations 2003, known as PECR. The most notable impact of PECR is the requirement for specific consent for electronic communications, such as email marketing, SMS marketing and automated calls. The new ePrivacy Directive is planned to be completed quickly so that it can go into effect around the same time as GDPR.

The Key Terms & their Definitions

Personal Data, Data Subject and Natural Person

Before GDPR

Under the Data Protection Act 1998 the term ‘data subject’ means a living individual who is the subject of personal data.

‘Personal data’ means data that relates to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or likely to come into the possession of, the data controller.

It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Changes under GDPR

Under GDPR the term ‘natural person’ replaces ‘data subject’ and there is a much broader definition of 'personal data' which includes various forms of personal or online identifiers:

‘any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.’ (Article 4)

The Key Terms & their Definitions

What about IP Tracking?

There is already a significant debate about whether IP addresses constitute personal data under this definition. Various regulators and court cases have asserted that this is the case but further clarification will be required on this point which could have huge ramifications for the online advertising industry.

Does 'Natural Persons' apply to B2B?

While companies are not 'Natural Persons', individuals who work at those companies are, so the GDPR will apply equally to consumer and business-to-business data.

The Key Terms & their Definitions

Data Processing

Before GDPR

Under Data Protection Act 1998, 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, including:

- 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, or
- Alignment, combination, blocking, erasure or destruction of the information or data.

Changes under GDPR

Processing means: *'any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.' (Article 4)*

This definition is very broad and is likely to encompass the vast majority of business activities which use personal data.

The Key Terms & Their Definitions

Data Controller

Before GDPR

Currently the term 'data controller' means 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.

Changes under GDPR:

The term 'data controller' is a little more specific:

'the natural or legal person, public authority, agency or any other body which alone or jointly with others, determines the purpose and means of the processing of personal data where the purposes and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or Member State law.' (Article 4)

In effect, the organisation which collects and processes the data will be the 'data controller' and has the main responsibility for compliance and accountability for the data it holds.

The Key Terms & Their Definitions

Data Processor

Before GDPR

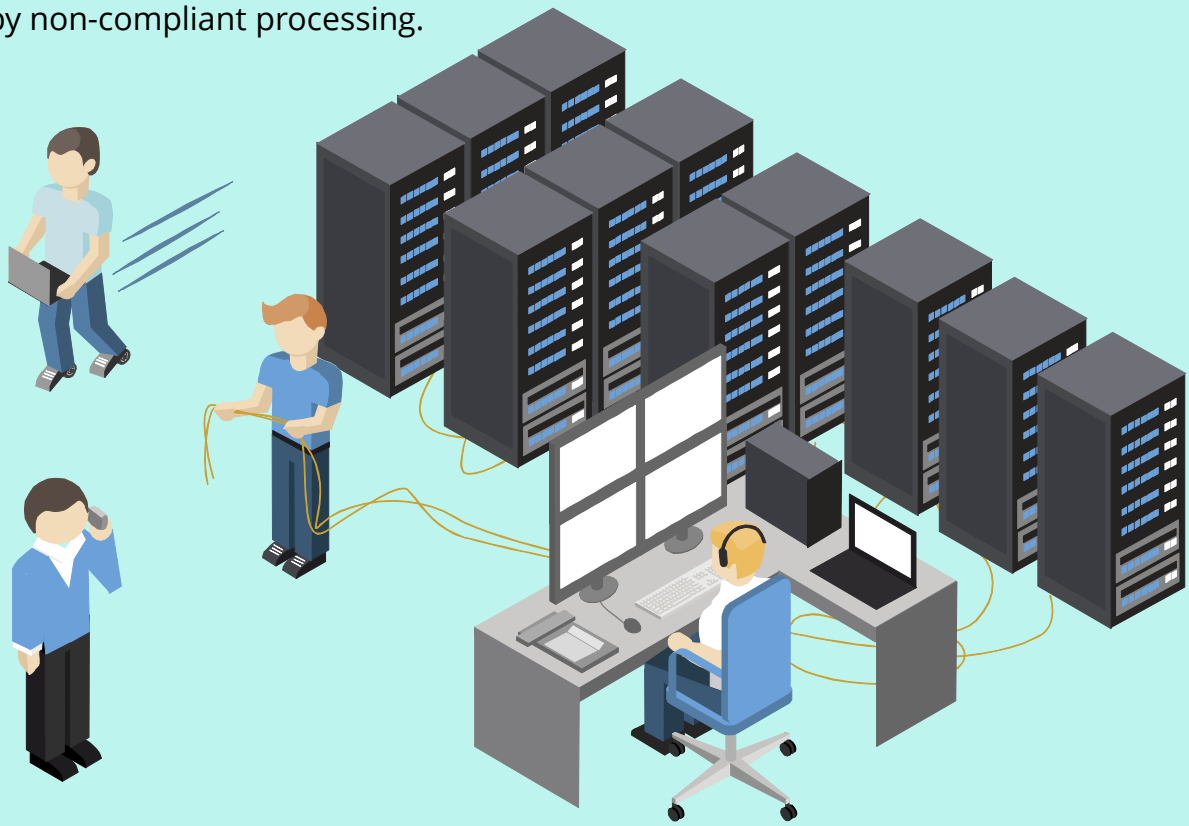
Under Data Protection Act 1998 'data processor' means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Changes under GDPR

Under GDPR, 'Processor' means:

'a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.' (Article 4)

There are new requirements in GDPR designed to make processors share the accountability for data protection compliance. They will also, for the first time, be jointly liable for breaches which require compensation of individuals for damage caused by non-compliant processing.



The Key Terms & Their Definitions

Special Categories of Personal Data (formerly called 'Sensitive Data')

Special categories of data are afforded extra protection under GDPR. These categories will, in most cases, require explicit consent for processing.

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Genetic data (new)
- Biometric data (new)
- Data concerning health or sex life
- Sexual orientation

Member State law will control processing of data about criminal record.

As under the current Data Protection Act 1998, there is a narrow exemption regarding the processing of special categories of data for non-profit organisations. However, this is unlikely to allow such organisations to process sensitive data in pursuit of fundraising.

Principles

The principles for protection of data stated within GDPR are not really very different from those under the Data Protection Act.

They are:

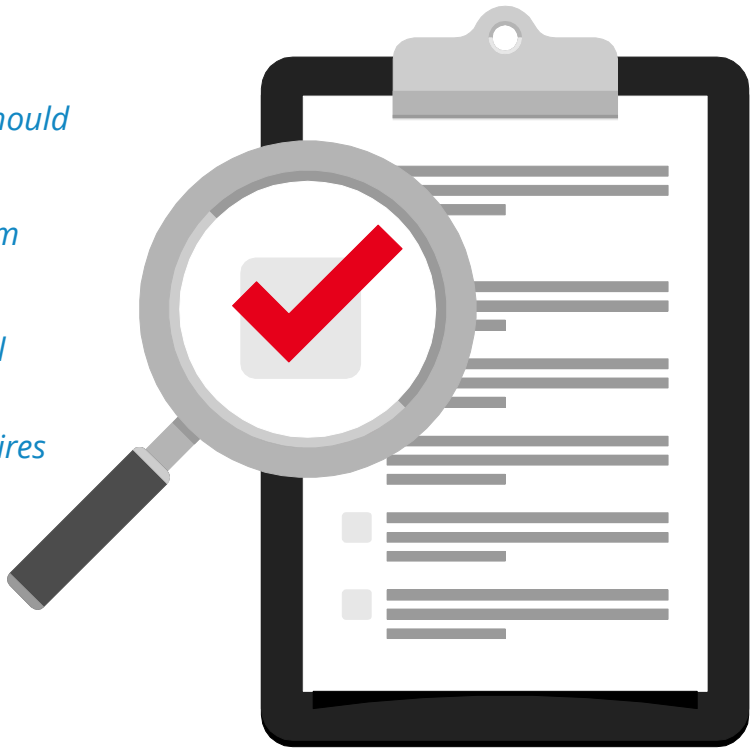
- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Data accuracy
- Storage limitation
- Integrity and confidentiality (security)

The themes of transparency and accountability come out strongly throughout the GDPR text.

Transparency

'Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.

The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.



Principles

That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed.' (Recital 39)

This requirement will have a significant effect on the way that organisations inform individuals of how their data will be processed. It will not be acceptable to hide information away in a densely written privacy policy or terms and conditions; the GDPR is clear that if consent is given without full transparency about the impacts of processing, it will not be valid.

Accountability

'The controller shall be responsible for and be able to demonstrate compliance with [the principles]…("accountability")'. (Article 5)

39 of the 99 articles require evidence to demonstrate compliance. There will be no requirement to notify processing to the Supervisory Authorities under GDPR but organisations (especially larger businesses) will need to keep detailed records of their processing.

What Makes Processing Legal?

In practice there are six ways in which lawful processing of personal data may be carried out. These are where processing:

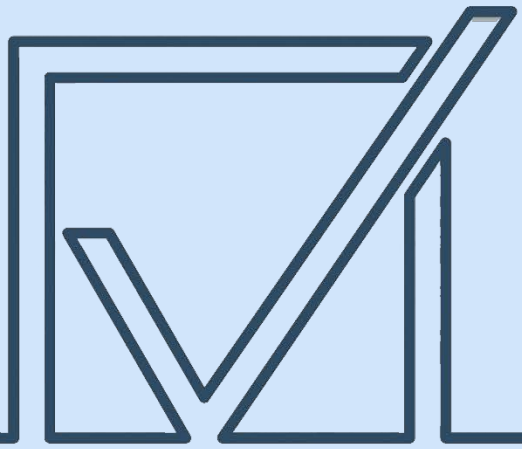
- Is necessary for performance of contract
- Is in compliance with legal obligation
- Is necessary to protect vital interests of the data subject
- Is in the public interest or exercising official authority
- Is with the consent of the natural person
- Is in the legitimate interests of the controller, or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the natural person.

'In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity 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.' (Recital 40)

These conditions are very similar to those in current legislation but ensuring they are correctly applied is vital. Processing in pursuit of a contract is probably the most straightforward; it will be transparent to an individual that their data will be processed in order to deliver goods and services.

However, any further use of data (including follow up marketing) will need to meet one of the other conditions for processing. We will now look in depth at processing under the grounds of Consent and Legitimate Interests.

Consent



Under Data Protection Act 1998, consent is defined as 'Any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'.

The definition of consent has been changed under GDPR. The data subject's consent means:

'any freely given, specific, informed ***and unambiguous*** *indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.' (Articles 4 & 32)*

There has been much debate about the meaning of the word 'Unambiguous' and whether it means the same as 'Explicit' and therefore would require 'opt-in'.

In a dictionary they appear to be very similar.

Steve Wood of the Information Commissioner's Office has said: *"If you read the recitals there is not much difference between 'unambiguous' and 'explicit' "* and it is likely that the Supervisory Authorities in the rest of Europe will be looking for active rather than passive consent under GDPR.

The requirement for a "clear affirmative action" also points strongly at the need for opt-in consent.

Consent

The Articles and Recitals include some further information about how to interpret the requirements for consent, which are covered below.

As this is a key area of interpretation there will be further guidance from the authorities which will help businesses to ensure they are compliant.

Many websites currently pre use pre–ticked boxes to obtain consent but these will not be considered a valid form of consent under GDPR:

'Silence, pre-ticked boxes or inactivity should not therefore constitute consent.' (Recital 32)

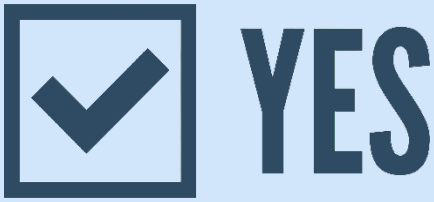
GDPR also makes it clear that consent should not be conditional upon sign-up to another service, i.e. bundled together. This technique is commonly used by UK organisations and may no longer be considered valid consent under GDPR:

'When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.' (Article 7)

Individuals must also be told they can withdraw consent and it must be simple to do.

'The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.' (Article 7)

Consent



Parental consent for processing

The age at which young persons are empowered to give consent to process their personal data is one of the things derogated to Member States laws. The standard age at which consent may be given by the individual is 16 years. Parental consent will be required for young persons in the EU under that age unless their Member State has set a younger age in local law. The minimum age a Member State may set is 13 years.

Is there a time limit to consent?

Under Data Protection Act 1998 there is no fixed time limit at which consent for processing expires and this does not change under GDPR. However, current guidance from the ICO says that context is important and it should be assumed that consent does not remain valid forever. An important thing to note is that a person's most recent indication of consent is paramount – if a customer agrees to marketing on three previous occasions but opts-out the fourth time, it is this last decision that must be applied.

GDPR does require that individuals are given information about how long their personal data may be processed (see below Information to be provided to Individuals).

Consent

Proof of consent

Organisations that are processing data with consent will have to be able to demonstrate they have obtained consent fairly and that the individual was given the necessary information to understand their choices:

'Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and the extent to which consent is given.' (Recital 42)

In practice this means having some way of recording on the database the details of the consent which has been gained, e.g. the type of consent, purposes of use that were stated, date gained, etc.

Most businesses will struggle to accommodate the detailed records which may be needed under GDPR on current systems and development may be needed.

Data controllers will have to decide whether they will record consent by channel (regarded as best practice but not an absolute requirement of GDPR).

The date a consent was given should be recorded as well as the mechanism used to obtain consent (online clicks or positive agreement on the telephone for example).

Actual wording used at the time consent was obtained will also need to be provided if there is a challenge to the validity of the consent.

Processing Under ‘Legitimate Interests’

There is an existing provision under Data Protection Act 1998 for the processing of data where it is in the ‘Legitimate Interests’ of the data controller to do so. It may also be used by third parties to whom the data controller has disclosed the data.

Much of this flexibility has been maintained under GDPR. To summarise a large amount of text within GDPR, the data controller must be able to demonstrate that their own legitimate interests to process personal data are not overridden by the interests or fundamental rights and freedoms of the data subject.

This is another area where interpretation will be important. Organisations may be tempted to rely on this condition for legal processing because the barrier for consent will be so much higher under GDPR. There are, however, conditions which must be met in order to make a proper assessment of whether the “balance of interests” in favour of the data controller is fair.

Processing must be within the ‘reasonable expectations’ of data subjects.

‘The legitimate interests of a controller, including of a controller to which the data may be disclosed, or of a third party may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on the relationship with the controller.’ (Recital 47)

Processing Under ‘Legitimate Interest’

It may be used to process data of employees or clients:

‘A legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.’ (Recital 47)

For preventing fraud:

‘The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned.’ (Recital 47)

The data controller should keep a record of the careful assessment of legitimate interests and this should be documented and stored.

‘At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.’ (Recital 47)

Public authorities cannot use the legitimate interest route, nor can organisations process the personal information of children.

Processing Under 'Legitimate Interest'

Using Legitimate Interests for Direct Marketing

'The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.' (Recital 47)

This Recital 47 (above) apparently contains great news for marketers. But it should be remembered that electronic communications must still meet the requirements under the Privacy & Electronic Communications (EC Directive) Regulations, 2003 - known as PECR.

These require electronic communications such as email, text messages or automated phone calls have to have specific consent.

Therefore for direct marketing purposes, the condition of legitimate interests is limited to direct mail and telephone calls, and those calls must be screened against the Telephone Preference Service (TPS) and Corporate TPS (CTPS).

Individuals must be informed that their data is being processed under legitimate interests. Organisations may wish to use the Privacy Policy to notify them.

In practice this is rather challenging, as it is not going to be easy finding the right words to explain in a customer-friendly way that the organisation is choosing to process their data based on legitimate interests.

Individuals also have the right to object to this type of processing.

A controller that relies on 'legitimate interests' for data collection must have a record to show that proper consideration has been given to the rights and freedoms of data subjects.

Profiling

There is no definition of 'profiling' under existing data protection law. Under Data Protection Act the only protection afforded is the right to challenge automated decision making.

Under GDPR profiling has been given a comprehensive definition, which is intended to include all forms of automated decision-making:

'Such processing includes also 'profiling' consisting in any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.' (Article 4)

During the negotiations of the GDPR text there was significant concern that all profiling (including that for marketing purposes) would be subject to the requirement for consent. In the final text, GDPR identifies two different types of profiling.

1. Profiling with legal or similarly significant effects, i.e. profiling from which 'decision are based that produce legal effects concerning him or her or similarly significantly affects him or her'.

2. Other profiling without such effects (including most profiling for direct marketing purposes).

Profiling

Profiling with legal or similarly significant effects

This type of profiling is only allowed if one of these conditions is met. The decision (arising out of the profiling):

- Is necessary for entering into, or performance of, a contract between the data subject and a data controller ; or
- Is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- Is based on the data subject's explicit consent.

In practice, some profiling will clearly have significant effect on the individual. For example, a mortgage application is likely to have legal effects, i.e. you may get accepted or declined depending on the results of the credit assessment (profiling).

Mortgage providers will have to argue that such profiling is necessary for entering into a contract or, alternatively, obtain explicit consent from applicants.

Profiling

However, the words 'similarly significant' have not been explained further, so until any guidance is published there is some doubt as to what types of profiling may be included in this category.

The default position for profiling with legal effect is that it cannot be carried out unless one of the conditions is met. Article 22 says:

'The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.' (Article 22)

Where explicit consent is used as grounds for processing the individual must have the right to withdraw their consent, i.e. opt-out. They must also be informed of the consequences if they object.

Profiling for Direct Marketing Purposes

Profiling for direct marketing purposes is less controlled and explicit consent is not required. But there is still a right to opt-out. Article 21 says:

'Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.' (Article 21)

If an individual opts-out they must be excluded from future profiling for direct marketing purposes:

'Where the data subject objects to the processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.' (Article 21)

Profiling

Organisations will need to inform individuals that they are being profiled, on or before the time of the first communication, using explicit wording clearly and separately from other information.

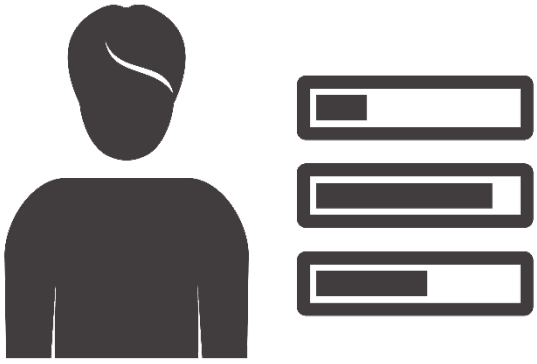
Example: Notification of profiling

"We may use the information you provide to us to better understand your interests so we can try to predict what other products, services and information you might be most interested in.

This enables us to tailor our communications to make them more relevant and interesting for you.

If you don't want us to do this you may opt-out here"

Profiling



Other new requirements for profiling

As now, the data subject has the right to obtain human intervention regarding a decision made wholly by automated means 'to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision.'

In addition and in order to ensure fair and transparent processing in respect of the data and taking into account the specific circumstances and context in which the personal data are processed, the data controller should use 'appropriate mathematical or statistical procedures' for the profiling.

The data controller should 'implement technical and organisational measures' appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised.

'In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.' (Recital 71)

The Rights of Natural Persons (Data Subjects)

Many of the existing data subject rights have been carried across to the GDPR, although the new Regulation makes some changes to those rights and adds some new rights.

Right to Object

The new Regulation retains the existing right for individuals to object to processing for direct marketing purposes, i.e. to 'opt-out' of direct marketing.

'Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether the initial or further processing, at any time and free of charge. This right shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.' (Recital 70)

It also gives a right to object to processing, including profiling:

1. *'The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions.*

The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.'

The Rights of Natural Persons (Data Subjects)

2. *'Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing'. (Article 21)*

Where processing is based on legitimate interests, the data controller must tell the individual and inform them of their right to object to processing on those grounds (Article 13).

All these rights will need to be communicated to consumers and, when they exercise their right to object, organisations will need the capability to act on those instructions. This may impact on the database and data management processes.

The Rights of Natural Persons (Data Subjects)

Right of Access: Subject Access Requests

Individuals have the right to have access all the personal data stored on them. The information needs to be supplied in writing, or in electronic form when the request has been made electronically (unless it is requested in writing).

'A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided.' (Article 63)

The key changes in GDPR are:

- There will be no fee for the first copy of information in response to a subject access request. Data controllers may charge if the individual asks for a copy to be sent to another interested party, e.g. their solicitor.
- There is a shorter deadline of one month (it is currently 40 days under the Data Protection Act). The timescale may be extended by two further months if it is a particularly complex request.
- The change to 'no fee' may well lead to a rise in the number of requests which controllers receive.

The Rights of Natural Persons (Data Subjects)

The information which needs to be included within an access response can be significant.

Along with the purposes of the processing, and the categories of personal data that have been collected, the controller must also supply the following information:

- The recipients of the personal data, including those outside the EU
- How long the data will be stored
- The right to request rectification or erasure of personal data
- The right to object to processing
- The right to complain to the Supervisory Authority
- Knowledge of personal data still undergoing processing, along with its significance and consequences.

The Rights of Natural Persons (Data Subjects)

If an organisation receives a Subject Access Request, proof of ID from the data subject should be requested. It is possible to ask what specific information the individual wishes to see, as this may help to reduce the scope of the task, but if the individual refuses to limit the request, all personal data being processed must be provided. Article 12 provides for instances where requests are 'manifestly unfounded or excessive'.

'Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request..' (Article 12)

Right to Rectification

If a data subject finds any inaccuracies in their personal data they can ask the organisation to rectify it.

'The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement..' (Article 16)

The Rights of Natural Persons (Data Subjects)

The Right to Erasure

The existing right to be forgotten has been extended into the right to erasure. This gives natural persons the right to request their personal data to be erased 'without undue delay'.

Article 17 reads as follows:

'1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- *the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing of the data;*
- *the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;*
- *the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);*
- *the personal data have been unlawfully processed;*
- *the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;*
- *the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).)'*

The Rights of Natural Persons (Data Subjects)

Naturally there will be instances where erasure of their data would not be appropriate. These are summarised below.

- For compliance with a legal obligation to a Union or Member State law.
- Exercising the right of freedom of expression (the processing of personal data carried out for journalistic purposes or the purpose of artistic or literary expression)
- Reasons of public interest in the area of public health (such as cross-border health threats)
- For historical, statistical and scientific research purposes

Quite a few eventualities may be included within compliance with a legal obligation, for example, where the individual has an outstanding debt to the controller.

Controllers must inform any other data processors of any erasure request and take "reasonable steps" to tell other data controllers of the request where the data has been shared.

When complying with an erasure request data controllers may retain a minimal amount of the individual's personal data for suppression purposes only:

'However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.' (Recital 65)

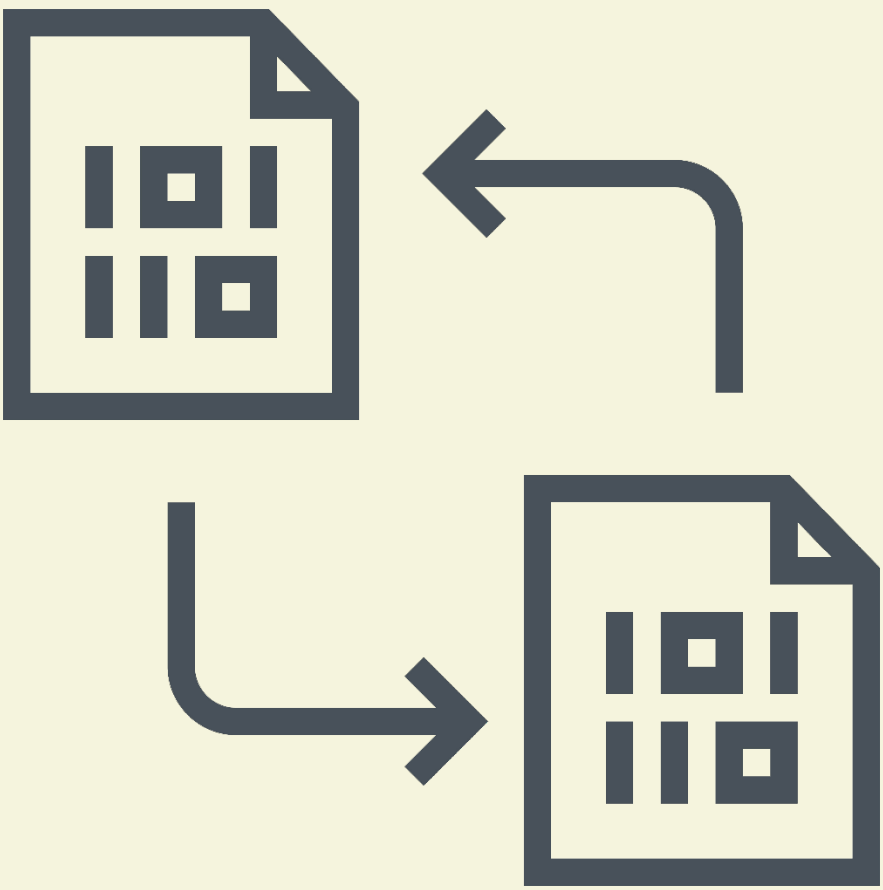
In this circumstance the data stored should be reduced to the bare minimum required in order to suppress the data from being used again. GDPR sets out the ways in which companies may comply with erasure requests.

The Rights of Natural Persons (Data Subjects)

'Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website.

In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.' (Recital 67)

If the data controller uses regular data feeds from third parties, it will need to take steps to ensure that the individual's data in not loaded and processed again. So in practice this means it should screen third party feeds against this new suppression file.



The Rights of Natural Persons (Data Subjects)

The Right to Data Portability

Under GDPR there is a new right to data portability, designed to make it easier for individuals to switch between service providers, e.g. utilities, financial services, etc.

'To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. ' (Recital 68)

This applies when the processing is based on consent, or the data is necessary for the performance of a contract and the processing is carried out by automated means. So it does not apply when processing data under any other grounds, e.g. Legitimate Interests.

'That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract.' (Recital 68)

There appears to be some flexibility in this area, as shown in Recital 68:

'Where technically feasible the data subject should have the right to obtain that the data is transmitted directly from controller to controller.'

'Data controllers should be encouraged to develop interoperable formats that enable data portability' but this does not create an obligation for the controllers to adopt or maintain data processing systems which are technically compatible.'

'The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible.'
(All from Recital 68)

There is no mention of any requirement to check it has been received successfully and that it can be processed by the receiving controller.

Information to be provided to individuals

At the time the data is collected directly from individual the following information must be provided:

- Who is the data controller?
- Their contact details
- What are the purposes of processing?
- Are Legitimate Interests being relied upon by the controller or third parties?
- Who the recipients of the data may be
- If the data will be transferred outside the EU and how this is protected
- How long will it be stored?
- How to exercise rights
- The right to withdraw consent
- The right to complain to the Supervisory Authority
- Whether data is required for contractual purposes and the consequences of refusing
- Whether profiling with legal effect exists

Where data is collected from third party sources (i.e. list rental), all the above shall apply PLUS the individual must be notified from which source the personal data originates and, if applicable, whether it came from publicly accessible sources.

An individual must be told within a month or when data is used to communicate or if a further disclosure is made unless they already have the information or it may be demonstrated that it would involve “disproportionate effort”.

Data Collection Notices Examples

The practical impact of GDPR on data collection statements will be significant.

The need for overall transparency, and the new requirements to inform individuals of profiling and their right to object, will need careful wording.

Here are some example data collection statements to help illustrate how these changes might look within a data collection statement.

Notification and consent for legal profiling; consent for marketing

The information you provide may be used to assess your application and your ability to re-pay our loan.

We may also use information provided by credit reference agencies and other loan providers. Please tick here [ ] to agree to this use of your information.

Please indicate how we may contact you with special offers and information about our other products and services:

☐ I'd like emails

☐ I'd like you to mail me

Consent, notification of profiling, right to object to DM and to profiling

At ACME, we have exciting offers and news about our products and services that we hope you'd like to hear about. We will use your information to predict what you might be interested in. We will treat your data with respect and you can find the details of our Contact Promise here.

☐ I'd like to receive updates from ACME based on my details

You can stop receiving our updates at any time and if you prefer that we do not use your information to predict what you might be interested in let us know here.

Consent, notification of profiling, right to object

At ACME, we have exciting offers and news about our products and services that we hope you'd like to hear about. We will use your information to predict what you might be interested in. We will treat your data with respect and you can find the details of our Contact Promise here.

☐ I'd like to receive updates from ACME based on my details

You can stop receiving our updates at any time.

Data Collection Notices Examples

Notification and consent for legal profiling; consent for marketing

The information you provide may be used to assess your application and your ability to re-pay our loan. We may also use information provided by credit reference agencies and other loan providers. Please tick here [ ] to agree to this use of your information.

Please indicate how we may contact you with special offers and information about our other products and services:

☐ I'd like emails

☐ I'd like you to mail me

Notification and opt-out of profiling

ACME may use the information you provide to us to better understand your interests so we can try to predict what other products, services and information you might be most interested in. This enables us to tailor our communications to make them more relevant for as an individual.

If you don't want us to do this you may opt-out here

Data Protection Impact Assessments

There are currently no specific requirements to carry out assessments of the privacy impact of new data processing projects. The new regulations will make it mandatory for data protection impact assessments (DPIAs) to be carried out when an organisation is considering engaging in certain 'high risk' data processing activities. A DPIA aims to understand and address any privacy issues that might arise before the processing is undertaken.

By identifying and anticipating risks to data protection, privacy and security, a DPIA helps by:

- Improving the quality of personal data, service and operation processes and decision-making regarding data protection
- Preventing costly adjustments in process or system redesign and mitigating risks with an early understanding of major risks
- Improving the feasibility of a project
- Strengthening consumer confidence by demonstrating a respect for privacy.

Recital 35 explains when a DPIA may be required:

'Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.' (Recital 35)

Assessments must be carried out prior to processing to ensure that risks are mitigated and compliance with the Regulation is demonstrated. Assessments are not retrospective to the Regulation as long as there was compliance with the prior Directive.

Record Keeping

If a Controller or Processor has more than 250 employees detailed records of the processing undertaken need to be kept.

Smaller businesses are exempt unless the processing carried out carries a high privacy risk or involves sensitive data.

The records must cover:

- Name and contact details of the controller and their Data Protection Officer
- Purposes of processing
- Classes of data
- Details of recipients of data
- Overseas transfers
- Data retention periods (where possible)
- Security measures in place (where possible)

Data Protection Officers

Once GDPR is in force, some organisations will be required to appoint a Data Protection Officer (DPO), including:

- Public authorities that process personal data
- Entities whose 'core activities' involve 'regular and systematic monitoring of data subjects on a large scale'
- Entities whose 'core activities' involve 'large scale' processing of 'special categories of data'. For example, data relating to health, ethnicity, political opinion or religious beliefs
- Those already obliged by local law, even if none of the above applies.

For other organisations, appointment of a DPO will be optional.

Tasks of a Data Protection Officer

- Inform and advise the organisation and its employees of their obligations to comply with GDPR, as well as other Union or Member State data protection laws
- Monitor compliance with the Regulation and appropriate laws, including managing internal data protection activities, staff training, and conducting internal audits
- Provide advice where requested on data protection impact assessments
- Act as the organisation's contact point for issues relating to the processing of personal data
- Respond to individuals whose data is being processed on issues relating to data protection, withdrawal of consent, the right to be forgotten and other regulatory rights
- To cooperate with the supervisory authority

A parent company with multiple subsidiaries may be able to appoint a single Data Protection Officer, under the condition that they are 'easily accessible from each establishment'.

Again, the definitive meaning on 'easily accessible' has not yet been confirmed but it may be taken to mean someone who resides within the European Economic Area.

Data Protection Officers

Requirements relating to the DPO role

- Data controller must support the DPO and ensure he or she has the right skills
- The functions the role can be performed by either an employee or a third party service provider under a service contract, such as consultancy and legal firms
- Their contact details should be published to encourage contact from data subjects
- They will be bound by secrecy of confidentiality concerning the performance of their tasks
- They can fulfil other 'non-conflicting' tasks
- They must not receive any instructions regarding the exercise of his/her duties
- They shall not be dismissed or penalised for performing their tasks
- They shall directly report to the highest level of management
- They cannot be held personally liable in the context of a failure to perform their obligations.

Data Breaches

At present data breaches do not need to be routinely notified to the Regulator. Notification is optional, but often advisable if the breach will affect consumers.

GDPR makes informing the relevant people and authorities of a data breach imperative, especially when the breach may involve risks to individual freedoms.

A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Under GDPR, data controllers shall inform regulators 'without undue delay' and 'not later than 72 hours' that a breach has taken place. Should this notification not be made in time, then there must be 'reasoned justification' for the delay.

Along with the regulators, where a data breach is likely to be a high risk to the rights and freedoms of individuals, the company is also required to communicate the nature of the breach, in plain English, to the data subjects concerned, without undue delay.

'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.

Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay..' (Recital 85)

There are some circumstances when the notification to the data subject is not required, including:

- If the organisation has implemented protection measures in respect to the personal data affected by the breach (encryption, for example).
- If the organisation has taken subsequent measures to ensure that high risk to the rights and freedoms of individuals is no longer likely to arise.
- It would involve 'disproportionate' effort, although details of what can be considered disproportionate have not been made clear.

Controller and Processor Liability

Data controllers are currently required to bear full responsibility when there has been a failure to comply with data protection law. Data processors are generally only subject to obligations that a controller has imposed by way of contract.

GDPR has been designed to make it easier for consumers to claim compensation where they have suffered any damage, and any person who has as a result of an infringement has the right to receive compensation. Under the new rules both controller and processor can be held responsible for compensation of individuals for any damage (material or non-material) suffered.

'Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.' (Article 82)

Where both controller and processor are involved, each party shall be held liable for the entire damage. A controller or processor shall only be exempted if they can prove they are 'not in any way responsible'. If controller is defunct, the processor will be wholly liable.

'Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

A controller or processor shall be exempt from liability under paragraph 2 if it 'proves that it is not in any way responsible for the event giving rise to the damage.' (Article 82)

Controller and Processor Liability

Detailed written contracts need to be in place between controllers and processors. Sub-contractors must be notified to controllers and should be bound by same terms as the main processor.

Mechanisms will need to be put in place for resolving disputes to settle compensation claims.

Processors may request indemnity provisions to reflect their increased exposure to risk.

What should contracts contain?

- The nature of the processing, the categories of data and the term
- The rights and duties of each party
- Staff confidentiality
- Security of data
- Approval of sub-contractors
- Assistance in fulfilling data subjects' rights
- Assistance with conducting DPIAs and with Privacy By Design
- Processor must provide sufficient guarantees as to technical and organisational measures to ensure GDPR compliance data subject rights
- Deletion or return of data on termination
- Right to audit the processor
- Processor must "call out" any instructions from controller which could lead to a breach
- Standard contractual clauses may be drafted by the European Commission and Regulators.

Enforcement and Penalties

Currently, the Information Commissioner's Office (ICO) and equivalent data protection regulators in each European State handle the enforcement of data protection laws.

Regulators have the authority to name and shame companies that have transgressed, as well as impose fines – in the UK up to £500,000. Criminal prosecutions may also be made.

The monetary penalty regime under the GDPR is significantly more punitive.

Some of the more serious regulatory infringements (such as the unlawful processing of the personal data of a child under the age of 13, failing to maintain records of processing activities, insufficient data protection, failing to demonstrate consent, denying data subject rights, or failing to report a data breach, to name a few) can attract hefty fines.

Depending on the nature of the infringement, this could be a fine amounting up to:

- 2% of total global annual turnover, or €10 million (whichever is the higher)
- 4% of total global annual turnover, or €20 million (whichever is the higher)

What can organisations do now to prepare for GDPR?

GDPR CHECKLIST

1. Begin preparations NOW – don't wait for GDPR to come into force
2. Make sure privacy notices meet the "transparency" challenge
3. Assess the impact 'opt-in' would have on the database
4. Test and optimise data collection statements
5. Consider using legitimate interests for some processing
6. Make sure the database can store proof of consent and multiple permissions
7. Review contracts with processors
8. Check whether the type(s) of profiling your organisation conducts will need explicit consent
9. Prepare to fulfil the new rights of natural persons
10. Undertake a formal GDPR Impact Assessment

Glossary of GDPR Terms

Consent: Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by a statement or a clear affirmative action which signifies agreement to the processing of Personal Data.

Data breach: An occurrence which results in the security of Personal Data held by the Data Controller being compromised.

Data controller: A data controller is the organisation that collects personal data and decides how it will be used.

Data processor: A data processor is the organisation that processes personal data on behalf of the data controller.

Data Protection Impact Assessment (DPIA): A method of identifying possible risks to privacy from a specific processing activity.

Data Protection Officer (DPO): An individual or legal entity appointed to inform and advise the data controller or the data processor and the employees who carry out processing of their obligations under GDPR. Identifier: Information from which an individual could be identified.

Legitimate interests: Processing conducted in the interests of the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual.

Personal data: Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing: Any operation performed on personal data. This includes recording, structuring, storing and any form of analysis using personal data.

Profiling: Any form of automated processing of personal data used to make a decision about an individual. In particular to analyse a person's preferences, interests, behaviour, location or movements.

Right to erasure (to be forgotten): The right for data subjects to request their personal data to be erased 'without undue delay'.

Right to data portability: The right for data subjects to receive their personal data in a structured, commonly used and machine-readable format and to have it transferred to another data controller (e.g. when switching accounts).

Right to data subject access: The right for data subjects to ask a data controller to provide a copy (free of charge) of all the personal information being processed about them.

Special categories of data: Personal data about racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership; genetic data; biometric data; data concerning health or sex life; sexual orientation.

Supervisory Authority: An independent public authority which is established by a Member State to enforce the GDPR.

Maximising Permissions

Permission to market to your customers is a legal necessity and a commercial imperative. If you are experiencing low permission rates at sign-up, your data collection wording is not doing the job.

PermissionMax enables you to test variations so that you can optimise permission rates. All existing data collection statements tested benefit from a compliance review by data protection specialists, Opt-4. We will also advise you and provide alternative wording for testing, designed to optimise consent and reflect your brand's tone of voice.

Our online research panel provides essential feedback on whether your wording hits the mark and demonstrates clear and compelling reasons to give consent. The panel can predict opt-in rates for your brand and engagement by channel. We can also pre-profiling the panel to match your existing customer base, or specific audiences, allowing surveys to be finely targeted.

Uniquely, PermissionMax allows you to validate results by using our virtual focus groups to add qualitative commentary from your brand's advocates (and detractors). Our expert panel, curated by DQMGRC, will be your "critical friend", commenting on positive and negative aspects of proposed wording and answering your bespoke questions. Finally, we can get reactions to different creative treatments – including icons – by reproducing the look and feel of your consent statements for review by the panel.

Key Features

- Test existing wording against bespoke copy from our permission experts
- Closely replicates live testing by taking account of your brand profile
- Clear quantitative reporting with qualitative feedback
- Benchmarks consent by type and channel
- Qualitative results from an expert panel
- Feedback on creative execution and user experience

Benefits

- Provides actionable results
- Improves permission rates and revenue potential
- Ensures wording is compliant and future proofed
- Captures sentiment and gauges empathy

Deliverables

Opt-4 will test up to 4 permission statements for you in each wave of testing. Larger organisations may wish to conduct more than one wave to refine the statements further, particularly if you wish to evaluate varying statements by brand/portfolio. These statements can have different copy to cover multiple contact channels and may have a combination of opt-outs and opt-ins to suit your needs.

- Our methodology is to use an email survey to an audience which is balanced to match a UK profile. If you prefer we could tailor the profile to match your audience.
- Our survey asks 25 questions, designed to understand if consumers would give their permission, along with their thoughts and opinions on the statements in terms of trust, clarity, security and control.
- We anticipate approx. 500 survey responses to each wave, to give clear, robust results.
- Opt-4 will provide a written report which may be presented face to face or via conference call.

For more details please contact Opt-4 via Rosemary Smith on rosemary.smith@opt-4.co.uk or Simon Blanchard on simon.blanchard@opt-4.co.uk.

Useful Resources

The full GDPR text:
http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

The ICO's DP Reform website:
http://dpreform.org.uk/

ICO's 'Overview of the GDPR'
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Data Protection Network website:
www.dpnetwork.org.uk/gdpr

Data Protection Community group on LinkedIn:
https://www.linkedin.com/groups/8222427

About Opt-4

Opt-4 is a specialist data protection consultancy.

Opt-4 directors have held key positions within the UK DMA and continue to advise on data protection matters.

Opt-4 runs data protection courses for the Institute of Direct Marketing.

We keep a watching brief on privacy legislation in Europe and beyond to ensure advice is as 'future proofed' against changes in regulation as possible. Opt-4 maintains membership of the Federation of European Direct and Interactive Marketing.

www.opt-4.co.uk

About Blue Sheep

Since 1986, Blue Sheep has been creating marketing solutions to meet our client's B2B and B2C challenges, with a breadth of talent and experience that has helped maintain its position at the forefront of the database, insight and analytics market, as well as become a respected name for multichannel software solutions and Single Customer View databases.

Blue Sheep has worked with a number of well-known brands from a wide variety of verticals, including finance, government, hospitality, media, retail, technology and online gaming. Some of our clients include De Vere, Wyndham, UBM, Misco, RAC, Travelodge, CapitalOne, Liverpool Victoria and many more.

www.bluesheep.com

Disclaimer
The information provided and the opinions expressed in this document represent the views of the Opt-4. They do not constitute legal advice and cannot be construed as offering comprehensive guidance to the General Data Protection Regulation or other statutory measures referred to herein.