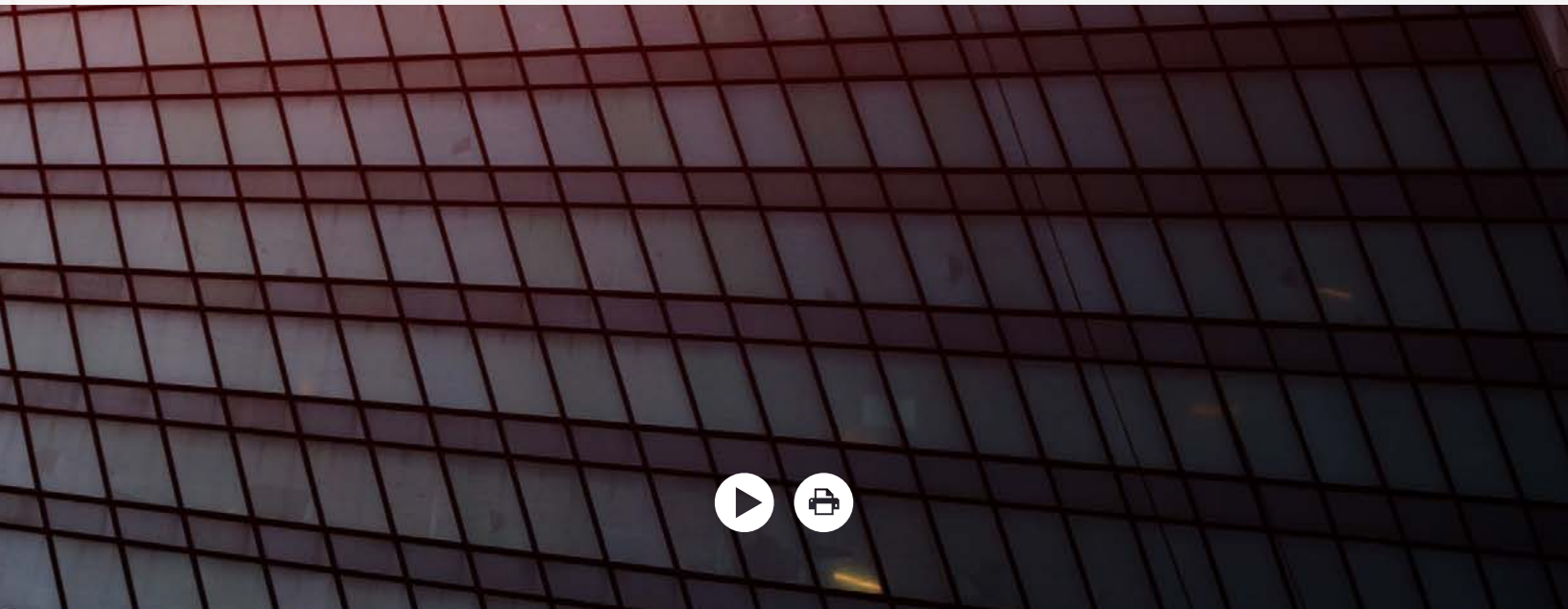
Global-Z

# THE GENERAL DATA PROTECTION REGULATION

A practical guide for global businesses.

MAY 25

MAY 25TH 2018
DEADLINE



Global-Z

MAY 25 MAY 25TH 2018 DEADLINE

***The General Data Protection Regulation (GDPR):*** A practical guide for Global businesses



Co-authored by Simon Blanchard and Karima Saini, edited by Rosemary Smith



# GLOBAL-Z FOREWORD

Companies that market to or collect data about individuals in the EU, including the UK, have new obligations that are being imposed beginning May 25, 2018.  This guide lets you jumpstart your preparation for the compliance journey. The European Union determined some years ago that it needed to develop a new Single Digital Market for the 28 Member States. In 2012, it began re-evaluating the 1995 European Union Data Protection Directive. This examination resulted in the 2016 General Data Protection Regulation (GDPR), which introduces elevated transparency, stricter consent rules, and prescriptive data governance obligations to enhance the privacy rights of individuals located in the European Union.

According to recent surveys, awareness and preparation for these new obligations is low. Global-Z commissioned European regulatory expert OPT-4 to prepare this guide. We hope this guide will help you prepare for the May 25, 2018 deadline.You may want to begin by referring to the 10 Steps to GDPR Readiness Checklist (Page 64).

*Ted Haas*

*Chief Marketing Officer*
*Global-Z International, Inc.*

* With the UK decision to conform to GDPR post 'Brexit,' these regulations will also apply to UK data subjects. EU Commission Directorate General notice to stakeholders on the UK withdrawal and the EU data protection rules. http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245

# CONTENTS



# INTRODUCTION

The world of data has exploded since the EU enacted the first Data Protection Directive in 1995. The Internet and E-mail for the general population were still in their infancy; social media as we know it today was not yet invented.


MAY 25TH 2018
DEADLINE

As the name suggests, the General Data Protection Regulation (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. This new piece of legislation was approved by EU Member States and will replace the 1995 Directive to enhance the data protection and fundamental privacy rights of all EU residents starting 25 May 2018.

Despite the UK decision to leave the EU (commonly referred to as 'Brexit'), the UK introduced its new Data Protection Bill on September 13, 2017. This bill will transfer the GDPR into UK law and be maintained to closely reflect GDPR after Brexit. Therefore, the principles laid down in the GDPR will be applicable to all UK organisations, and data subjects.

In any case, any businesses which market or monitor the activities of natural persons located in the EU, including the UK, will have to abide by GDPR.

The GDPR codified currently popular cross-border transfer mechanisms, including the Binding Corporate Rules (BCRs) used by multinational companies for inter-group data transfers. Although not expressly named, the EU-US Privacy Shield is contemplated within the GDPR framework on International cooperation for the protection of personal data.

The GDPR has 173 Recitals to help interpret the obligations set out in the 99 Articles (the 'Regulation').

*Note: Articles and Recitals extracted from the GDPR text are in blue italic.*

The European Data Protection Board (EDPB, currently known as The Article 29 Working Party) will continue to issue official guidance for organisations to refine and understand better ways they can meet their GDPR obligations in addition to those already released since December 2016. See the Resources section for a link to their official site.

# THE GLOBAL SCOPE OF GDPR

Non-EU organisations will be subject to the GDPR where they process personal data about natural persons located in the EU, 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.

Derogations under GDPR: There are certain requirements of the GDPR that may be derogated to local Member State law. There are more than 50 instances of potential derogations to local Member State law in the GDPR.

In Practice, this means the Regulation will not create a completely uniform regime throughout European Member States after all. For example, when a Data Protection Officer needs to be appointed, or at what age an individual would be classed as a child or an adult for enrolling in an information society service. In the UK, the Data Protection Bill 2017 that will replace the Data Protection Act of 1998 sets that age at 13 or older whereas other EU Member States may set that age anywhere up to 16 years of age.

European Data Protection Board Guidance: There are also instances where guidance can be provided by the newly created European Data Protection Board (formerly known as the Article 29 Working Party), or by local regulators. (See Resources for final guidance available to date.)

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.

# OTHER IMPACTFUL DIRECT MARKETING CONSIDERATIONS

When GDPR comes into force it will not stand alone as the only regulation affecting data-driven communications to individuals in the EU.

Today, each Member State imposes their own flavour of direct marketing rules using electronic messages and is the impetus behind the EU intending to also transform the current e-Privacy Directive into a new regulation. It will be aligned with the GDPR, including shared definitions and administrative fines and sanctions. As of the time of writing, however, the exact text and effective date of the new e-Privacy regulation have yet to be resolved.

The Resources provides a link to the latest version e-Privacy regulation plenary discussion draft issued on 20 October 2017 (consisting of 245 pages).

Marketers hope that the new regulation will allow direct marketing as a legitimate interest activity and not impose additional constraints or affirmative consent in all electronic communication use cases.  In many Member States, sending marketing messages via electronic communications (e-mail, SMS/Texts, fax and automated calls) requires consent.

The Certified Senders Alliance and the ECO Association of the Internet Industry have collaborated on useful booklets for e-mail Marketers (see Resource page) to understand some of these additional requirements. Considering the variances that can arise from future GDPR derogations combined with other online local laws applicable within various Member States, marketers are advised to consult local counsel to ensure compliance with all applicable rules, regulations, directives, guidance and regional industry best practices.

# THE KEY TERMS & THEIR DEFINITIONS

## Personal Data, Data Subject and Natural Person

**Before GDPR**

The UK's Data Protection Act 1998 defined a 'data subject' as a living individual who is the subject of personal data. 'Personal data' meant 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 included 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**

The GDPR clarifies the term 'data subject' by specifying that it relates to a 'natural person', and also expanded the definition of 'personal data' to include 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)*

**Does 'Natural Persons' apply to B2B?**

Yes. 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.

**What about IP Tracking?**

There had been significant debates about whether IP addresses constituted 'personal data' under that definition. Various regulators and court cases asserted that IP addresses are deemed 'personal data'; however further clarification is still sought on this point as it could have huge ramifications for the online advertising industry.

## Processing

### Before GDPR

Under UK's Data Protection Act 1998, processing, in relation to information or data, meant 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

The definition of processing is very broad and will encompass the majority of businesses handling personal data:

> *'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)*

## Data Controller

### Before GDPR

The term 'data controller' meant a person who, either alone or jointly or in common with other persons, determined 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 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 purpose 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, organisations collecting and processing personal data are the 'data controller' and will have the main responsibility for compliance and accountability for the data it holds.

### Data Processor

### Before GDPR

The UK Data Protection Act 1998 defined 'data processor' to mean any person (other than an employee of the data controller) who processed 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)*

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

### 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 before processing:

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

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

Although a GDPR exemption on the prohibition of processing special categories of data allows the use of 'personal data which are manifestly made public by the data subject', data controllers and processors will still be bound by other GDPR obligations such as conducting a data protection impact assessment to evaluate the potential use of such data against the fundamental rights and reasonable expectations of that individual. Reminder: laws other than GDPR may apply (see page 11 Other Impactful Direct Marketing Obligations).



### The GDPR and Accountability

Additionally, accountability comes out as a strong theme throughout the GDPR text and is unofficially referred to as the 'Seventh Principle'.

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

Thirty-nine 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.

# GDPR PRINCIPLES

**The Six GDPR Principles are:**

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Data accuracy
5. Storage limitation
6. Integrity and confidentiality (security)

**GDPR and 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.

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 transparency 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.

# FAIR INFORMATION PRACTICE PRINCIPLES & EU-US PRIVACY SHIELD FRAMEWORK

The GDPR permits transfers of personal data to third countries or international organisation when the third country, a territory or one or more sectors within that third country, or the international organisation in question ensures an adequate level of protection.



These transfers do not require any official, specific authorisation and include inter-company binding corporate rules (BCRs) and data controllers/processors standardised model contractual clauses.

The EU-US Privacy Shield Framework is an example of currently available cross-border data transfers mechanisms. It was built on the following internationally recognised Fair Information Practice Principles (FIPPs):

- Notice
- Choice
- Data Integrity and Purpose Limitation
- Access
- Accountability for Onward Transfer
- Security
- Recourse, Enforcement and Liability

The following chart reveals the similarities between the Six GDPR Principles and the Privacy Shield Framework:

| GDPR Principles | Privacy Shield Framework Requirements |
|---|---|
| 1. Lawfulness, Fairness and Transparency | • Notice to include type of data collected, right of access and choice, conditions for onward transfer<br>• Policies (reflecting principles) made public<br>• Inform data subject of available recourses to pursue against data controller<br>• Provide links to self-certification documents |
| 2. Purpose Limitation | • Notice to include purpose of processing |
| 3. Data Minimisation | • Limit personal data to what is necessary for the specified purpose of processing |
| 4. Data Accuracy | • Data for intended use must be reliable (complete, accurate, current)<br>• Protect data subject against adverse effects from automated decisions |
| 5. Storage Limitation | • Retained in an identifying way/identifiable only for as long as it serves the purpose of initial collection or subsequently authorized use (statistical analysis, public interest, journalism, scientific and historical research archiving principles apply) |
| 6. Integrity and Confidentiality (Security) | • Use reasonable and appropriate security measures taking into account the risk involved in processing and the nature of personal data |

https://www.dpnetwork.org.uk/gdpr-compliance-privacy-shield/

# WHAT MAKES PROCESSING LEGAL?

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

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.

> *'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)*

**Consent**

Under UK 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 UK 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.

GDPR includes 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 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)*

In practice, marketers will take the time left before the GDPR comes into force May 25, 2018 to review their customer lists for conformance with the new GDPR transparency, fair and lawful processing requirements.

Companies that want to ensure that they can send marketing messages to their current database client lists may develop a re-permission campaign.  Existing laws must be followed when designing such campaigns.

As a cautionary tale, be sure to consider all applicable laws in existence today before proceeding with well-intended permission campaigns to avoid negative press and penalties fines.  (In the UK, the data protection regulator recently fined Morrison's supermarket chain £10,500 for e-mailing supposed GDPR-proof marketing consent requests to 20,000 customers who had already unsubscribed from e-mail marketing. Higher fines from the UK regulator were imposed on Flybe (airline) and Honda on similar permission marketing e-mail campaigns.)

For data to be relevant, it should also be current, and has led some data governance advocates to advice companies to 'get rid of data that is past its sell-by date'.

YES NO

**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 UK regulator 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 page 46)

**Third Party List Rentals and GDPR**

The GDPR does not directly address the use of bought-in lists.

However, local data protection regulators may issue guidelines and the anticipated new e-Privacy Regulation in Member States to govern direct marketing via e-mail, telephone and other electronic communication channels.

As for 'bought lists', these list purchasers need to conduct due diligence on the list sellers to ensure that transparent, fair and lawful collection (GDPR Principle 1) occurred at the time the data subject completed the registration form or indicated affirmative consent to share their personal data with the intended list purchaser.

For data subjects located in the UK, the Information Commissioner's Office (ICO) has issued a Direct Marketing Checklist (see Resources). A few highlights from that checklist include these recommendations:

- We don't use bought-in lists for texts, e-mails or recorded calls (unless we have proof of opt-in consent within last six months which specifically named or clearly described us)
- The product, service or ideals we are marketing are the same or similar to those for which the individuals originally consented to receive marketing
- We screen the names on bought-in lists against our own list of people who say they don't want our calls (suppression list)
- We tie the seller into a contract which confirms the reliability of the list and gives us the ability to audit.

### 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'

The 1995 directive allows processing of personal 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. While much of this flexibility has been maintained under GDPR, a proper assessment must be performed to objectively determine whether the "balance of interests" in favour of the data controller is fair. Processing must also 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)*

In summary, a 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. Moreover, the availability of Legitimate Interests drastically diminishes and may even disappear if special categories (sensitive) personal data is involved.

The Data Protection Network (UK) has produced a free Legitimate Interests Assessment template and guide book for companies to adapt to their own circumstances and business vertical if they wish to conduct their own assessments (see Resources).

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 can only use legitimate interest route in limited circumstances, nor can organisations process the personal information of children.




**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 Member States may have electronic communications acts which must still be met. For the UK, these requirements are covered in the Privacy & Electronic Communications (EC Directive) Regulations, 2003 known as PECR. The rules will eventually be replaced by the e-Privacy Regulation.

These electronic communications regulations usually include e-mail, text messages and automated phone calls and most require specific consent from the individual before sending commercial messages.

In the UK, for direct marketing purposes, the 'legitimate interests' basis for processing is limited to direct mail and includes live telephone calls if the phone numbers are scrubbed against the long-established UK Telephone Preference Service (TPS) and Corporate TPS (CTPS) lists.

Additionally, individuals must be informed at the time the data is collected that their data is being processed under legitimate interests and that they have a right to object at the time of collection or easily any time later. Organisations may wish to point the reader to their GDPR-compliant Privacy Policy to learn more when they first notify them at time of collection.

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.

Data controllers may record their evaluation using a Legitimate Interests Assessment checklist prepared by The Data Protection Network in July 2017. It provides useful examples for 'Legitimate Interests'. (See Resources, DPNetwork.org.uk 'Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation' July.2017.)

# PROFILING

The GDPR has given a comprehensive definition of 'profiling', 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 types of profiling:

1. Profiling with legal or similarly significant effects, i.e., profiling from which 'decisions 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 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. However, the words 'similarly significant' have not been explained further, so until guidance is published there is some doubt as to what types of profiling may be included in this category.

The Article 29 Working Party has issued draft guideline for which it is seeking comments. Amended to guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679, wp251

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

> *'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. GDPR indicates that:

> *'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.'*

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)*

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.

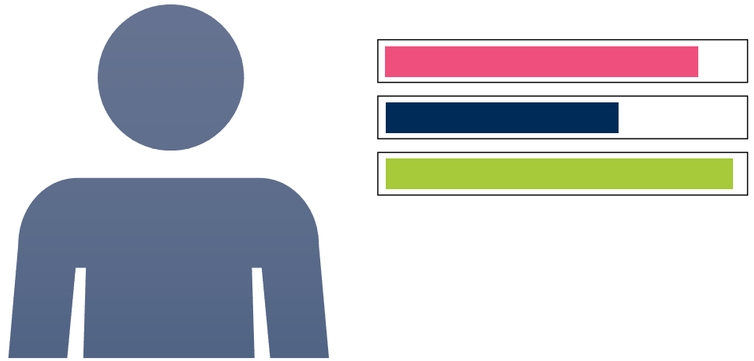
☐ If you don't want us to do this you may opt-out here"

### Other new requirements for profiling

As of 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)*

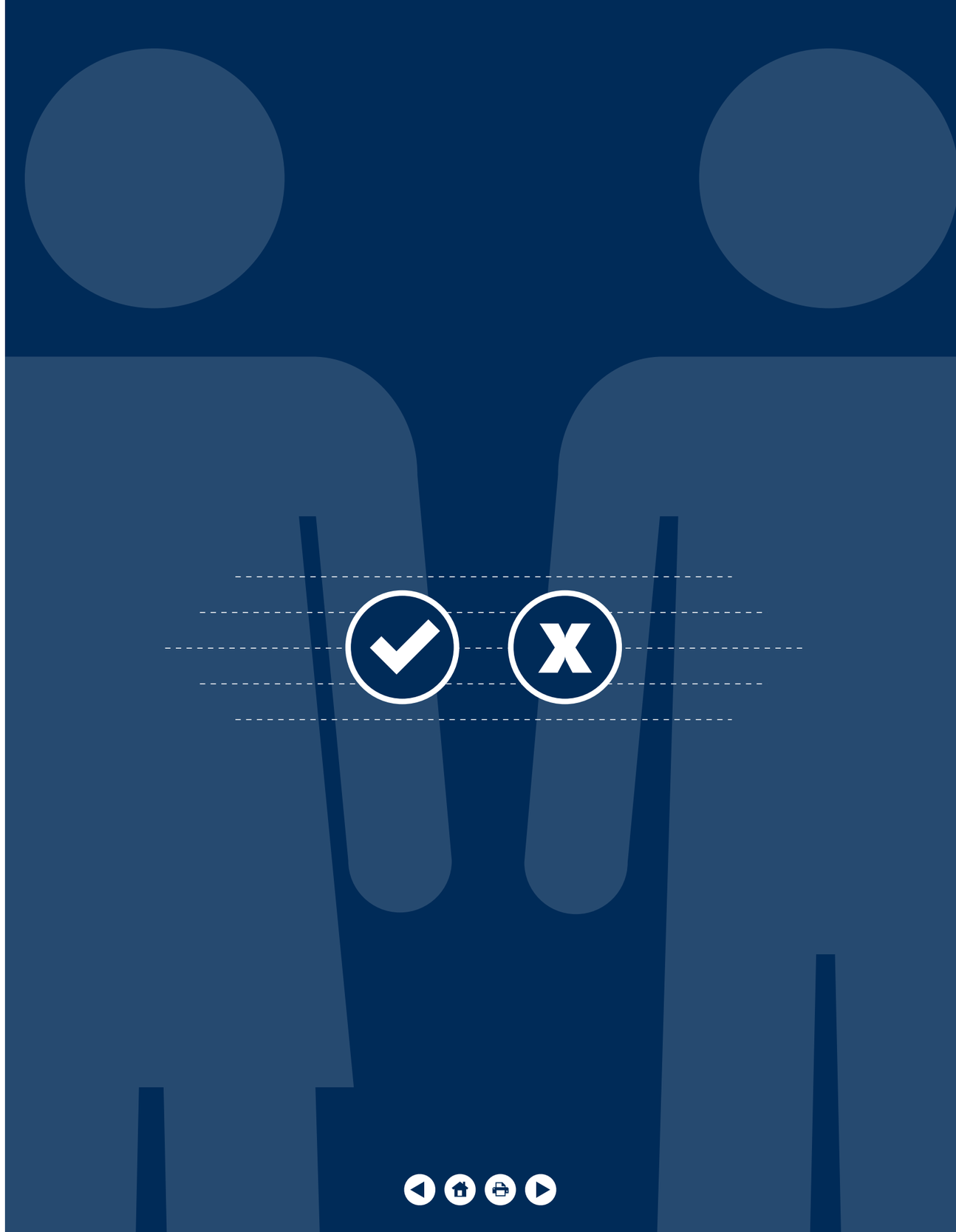
It also gives a right to object to processing, including profiling:

> *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 defense of legal claims.'*

> *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 individuals 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.





**Right of Access: Subject Access Requests**
Individuals have the right to have to 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.' (Recital 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 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:
    - o The recipients of the personal data, including those outside the EU
    - o How long the data will be stored
    - o The right to request rectification or erasure of personal data
    - o The right to object to processing
    - o The right to complain to the Supervisory Authority
    - o Knowledge of personal data still undergoing processing, along with its significance and consequences.



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 Right to Erasure

The existing EU 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 or the following ground applies:*
>
> *(a) 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; (c) 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); (c) the personal data have been unlawfully processed; (d) 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; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).*

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.




> *'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)*

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.

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.

> *'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 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 personal data is collected, directly, from the individual the following information must be provided:

- The identity of 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 data 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:

☐ You can unsubscribe from marketing emails any time

☐ I'd like you to mail me

**Consent, notification of profiling, right to object to Direct Marketing and 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.

**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 you as an individual.

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

# DATA PROTECTION IMPACT ASSESSMENT

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 individuals' confidence by demonstrating a respect for privacy

GDPR 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.

See Resources section for official Guideline on conducting DPIAs issued by Working Party 29.

Best practice tip: Consider having a basic 'gating' question at the start of any new project, purchase, system change, or new build that asks the question: Is there (or will there ever be) any personal information/data, sensitive personal data, or a way to identify an individual if the data at hand is or will be combined? If the answer is affirmative, conduct an internal privacy impact assessment (PIA) which only graduates to a DPIA if the outcome of the PIA enters the risk category described in Article 35.

# DATA GOVERNANCE

### 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 by the way of example:

- 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)
- Refer to the Excel templates for the full list published by the UK Information Commissioner's Office

### Record Retention

The GDPR "storage limitation" principle states that personal data be:

> *'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')' Article 5(1)(e).*

Data controllers (and processors if applicable) will need to include information about how long they retain personal data in their privacy statements to data subjects.

Privacy Notice Example, addressed in a section entitled "Data Retention; Storage & International Data Transfers" (at page 49)

Example Statement: Data Retention. We will keep personal information only for as long as we need it to maintain our relationship with you, provide you with the products, services or information you requested, to inform our research into the preferences of our customers, to comply with the law, and to ensure we do not communicate with individuals that asked us not to. When we no longer need the info, we will dispose of it securely, using speciality companies to do this work if necessary

# DATA PROTECTION OFFICERS

Once GDPR is in force, certain organisations must 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.

### Requirements relating to the DPO role

- Data controller must support the DPO and ensure he or she has the right skills
- The functions for this 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.

(See Resources for official guidance from the EU Article 29 Working Party)

# 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 individuals.

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 language, 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

The EU Article 29 Working Party has issued a preliminary draft guidance on breach notification with a request for comments to be returned late November 2017. Guidelines on Personal data breach notification under Regulation 2016/679, wp250

# CONTROLLER & 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 individuals to claim compensation where they have suffered any damage, and any person who, 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 (if liable) 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)*

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 of the GDPR
- Standard contractual clauses may be drafted by the European Commission and Regulators.

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.



# ENFORCEMENT AND PENALTIES

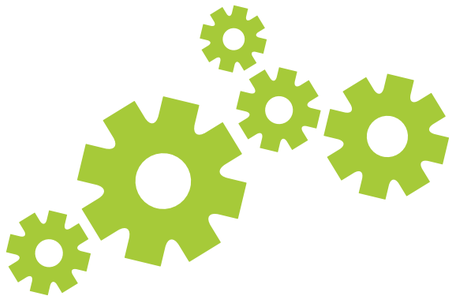
In the UK, the Information Commissioner's Office (ICO) and equivalent data protection regulators in each European Member State handle the enforcement of data protection laws. Regulators have the authority to name and shame companies that have transgressed, as well as impose fines –in the UK currently up to £500,000.

Criminal prosecutions may also be made in certain countries, such as in the UK.. 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)

(See a complete list, see *51 ways to get into trouble with GDPR* link in Resources)



# 10-POINT GDPR-READINESS CHECKLIST

**1. Who are your GDPR colleagues?**

Locate your internal GDPR stakeholders. Pro-actively identify colleagues working on the GDPR and collaborate with them.

**2. Do you really KNOW your data?**

Understand the EU personal data you have and why you process it. Analyse who, what, where, when and how personal data is/was collected and assess if you can keep using it compliantly under the GDPR.

**3. Can you rely on Legitimate Interests?**

The GDPR allows for direct marketing as a legitimate interest activity if certain conditions and a "balance of interests" test is met. Identify your marketing journeys, analyse whether a legitimate interest for direct marketing is available instead of consent, and if it is, record how you met the protection of individual's rights and reasonable expectations. [See DPN Legitimate Interest Guidance]

**4. Is your data collection compliant and effective?**

Ensure you tell individuals in easy to understand, plain language about your lawful bases for processing their data, give them choices, and respect their rights. Test your opt-in messages, including the new requirement to inform prior to the individual giving their consent. Ensure the right to easily revoke consent is offered. If relying on Legitimate Interests, inform them of their right to object.

**5. Is your Privacy Notice GDPR-ready?**

Post an updated privacy notice (policy) as soon as possible, so that data collected now can be used compliantly from May 2018 onward. The GDPR requires more detailed privacy notices, including how long you retain personal data, details of any sharing of personal data with third parties, an explanation of any profiling activities undertaken, how individuals can exercise their rights, where to send complaints and if non-EU countries will process personal data. [See the Information Commissioner's Office Privacy Notice guidance]

**6. Can your database evidence consent?**

Your systems must be able to store proof of consent and revocation, including granular communication channels. Ensure your (and any outsourced) systems can record consents and subsequent objections tied to specific purposes stated at time of collection associated with select communication channels (e-mail, text, mobile phone, landline, social media, etc.) [See DPN Processor Liability guide]

**7. Is data protection top of mind?**

Apply the principles of privacy by design to keep data protection for individuals top of mind from the moment you create, develop, modify, or buy products and services. Privacy-by-Design/Default means conducting data protection impact assessments, even consulting the data protection regulator if residual high risks to individuals are likely (e.g., profiling operations, or processing large quantity of sensitive personal data). [See UK Information Commissioner's Office (ICO) Privacy by Design principles and the UK Data Protection Network 'Data Governance' guide.]

**8. Does your data travel abroad?**

If personal data is processed outside the EU/EEA, make sure that the entity in the destination country has adequate mechanisms in place to protect EU-based individuals. Review your inter-company agreements and data processor contracts for cross-border data transfer mechanism that meet GDPR (binding corporate rules, US-EU Privacy Shield, EU model contract clauses, etc.]

**9. Is your staff "privacy aware"?**

Train your staff about the importance of data privacy and to promptly report any policy inconsistencies. Everyone has a role to play in safeguarding and respecting the personal data of their colleagues, clients, and business contacts so deploy training to new hires and regularly to all members of staff.

**10. Are you tracking data privacy news?**

Monitor your compliance program and keep abreast of new privacy laws. Watch out for the publication of regulatory guidance and keep an eye out for updates on the promised EU e-Privacy Regulation governing electronic communications.

# 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.

**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.



# USEFUL RESOURCES

**Introduction to The EU and the Digital Single Market**
https://publications.europa.eu/en/publication-detail/-/publication/8084b7f3-6777-11e7-b2f2-01aa75ed71a1

**Just for Small Enterprises: EU interactive quick FAQ**
http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_en.htm

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

**Adopted EU guidelines as of December 2017:**

1. Guidelines on Data Protection Officers ('DPOs'), wp243rev.01
2. Guidelines on The Lead Supervisory Authority, wp244rev.01
3. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01

**The e-Privacy regulation plenary discussion draft issued on 20 October 2017**
https://iapp.org/media/pdf/publications/Lauristin-report-ePrivacyRegulation-Oct2017.pdf

**Privacy Trust explanation of Privacy Shield Principles explained:**
https://www.privacytrust.com/privacyshield/principles/

**EU-US Privacy Shield:**
https://www.privacyshield.gov/article?id=Requirements-of-Participation

**The UK Information Commissioner's Office Data Protection Reform website:**
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

**The UK Information Commissioner's Office 'Overview of the GDPR':**
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

**The UK Information Commissioner's Office Data Protection Privacy and Electronic Communications 'Direct Marketing Checklist' v. 2.0:** https://ico.org.uk/media/for-organisations/documents/1551/direct-marketing-checklist.pdf

**The UK Information Commissioner's Office fines:**

1. Morrison's https://www.theregister.co.uk/2017/06/16ico_fine_morrisons_unsolicited_e-mails/

2. Flybe and Honda https://ico.org.uk/abouttheiconewsandeventsnews-and-blogs/2017/03/ico-warns-uk-firms-to-respect-customers-data-wishes-as-it-fines-flybe-and-honda/

**ECO Association of the Internet Industry,** www.eco.de **publication entitled 'eco Directive for Permissible e-mail Marketing: Guidelines for Practical Use' in Europe:** https://certified-senders.eu/documents

**Data Protection Network website:**
www.dpnetwork.org.uk/gdpr & '51 ways to get into trouble with GDPR' article at https://www.dpnetwork.org.uk/opinion/gdpr-51-ways-to-get-into-trouble-with-the-gdpr/DPNetwork.org.uk
'Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation' (July 2017)

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

**e-mail Marketing: Guidelines for Practical Use' in Europe:** https://certified-senders.org/wp-content/uploads/2017/07/Marketing-Directive.pdf

# ABOUT GLOBAL-Z.

Global-Z International delivers customer identity resolution and data quality solutions for some of the world's most well-known enterprises.  Our global expertise enables our clients to create a Single Customer View and to build the Golden Master Record across databases and national boundaries.  Our solutions are deployed for marketing, CRM migration, and master data management needs. Global-Z International, Inc., was founded in 1989 and is headquartered in Bennington, Vermont with offices and operations in the US, Canada, and Japan. We are both EU and Swiss Privacy Shield Certified.

**Disclaimer**

The contents of this paper are intended to convey general information only and not to provide legal advice or opinions. Global-Z does not accept any responsibility or liability for the accuracy, content, completeness, legality, or reliability of the information.  We urge all companies to contact appropriate legal counsel.

# ABOUT OPT 4 LTD.

Opt-4 has followed the development of the GDPR from the outset and has contributed to consultations by the ICO and Government on the impact for businesses. We also assisted in formulating submissions to Government from the UK Direct Marketing Association, the Advertising Association and FEDMA. We carry out GDPR Impact Assessments which test businesses readiness and alert senior management to significant compliance and revenue effects. Opt-4 has been selected by the UK Institute of Direct and Digital Marketing to develop and deliver face to face and online GDPR training. Over 500 delegates have attended the courses. Opt-4 runs the Data Protection Network website which provides useful resources for GDPR compliance.

**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.

Opt-4 Ltd. Registered office; Boundary House, Boston Road, London, W7 2QE. Registered in England 05290958, VAT Registration 851 0374 48.



BETTER DATA. BETTER DECISIONS.

Global-Z

Privacy Shield
Protecting your data

395 Shields Drive, Bennington, VT 05201 USA - globalz.com - info@globalz.com - **+1 802.445.1011**