
# ITSPA GDPR Guidance

February 2018

## Introduction

This guidance note sets out a summary of:

- The new regime including key terms, who must comply and the implications of failing to comply;
- Practical steps to be taken to achieve compliance;
- The implications of Brexit.

**Remember**:

The approach required will vary between businesses and these guidance notes are designed to be a summary of the GDPR requirements and steps you can take to become compliant. You should seek legal advice for tailored advice relating to the processing undertaken by your business.

This guidance is intended to help ITSPA members ("**you**") be aware of your regulatory obligations with respect to data protection in the UK. The General Data Protection Regulation ("**GDPR**") will significantly change and update the data protection regime across the EU. Your business will need to take steps to adapt and comply with the new regime. Taking action now will minimise the risk of the (increased) GDPR sanctions for non-compliance and reputational exposure and ensure that you have sufficient time for any implementation activities.

## What is the GDPR?

The GDPR is EU legislation governing the collection, use and storage of personal data and it will come into effect on **25 May 2018**. The GDPR constitutes the biggest change to the data protection regime in the EU since the 1995 Data Protection Directive implemented in the UK as the Data Protection Act 1998 ("**DPA**") and from 25 May 2018 it will replace the DPA.

The DPA must be formally repealed and the Government intends to do this through the Data Protection Bill ("**DP Bill**"). In addition to repealing the DPA, the DP Bill will set new standards for protecting general data in accordance with the GDPR e.g., by setting the age from which parental consent is not needed to process data online at age 13, preserve existing exemptions for research, financial services, journalism and legal services and provide a framework tailored to the needs of the criminal justice agencies and national security organisations.

The GDPR is not sector specific; there are no provisions that relate specifically to the communications sector. However, in this guidance note we have tried to highlight where there may be specific issues that communications providers should consider.

Other laws covering data and privacy issues will continue in force in addition to the GDPR:

- Privacy and Electronic Communications (EC Directive) Regulations 2003 ("**PECR**")* covering data (including traffic and location data and electronic communications services) and marketing;
- Call recording rules and data retention obligations under the Investigatory Powers Act 2016 ("**IPA**");
- Regulation of Investigatory Powers Act 2000 ("**RIPA**"); and
- Data Retention and Investigatory Powers Act 2014 ("**DRIPA**").

*PECR is derived from the European e-Privacy Directive and work has separately started to update it in the form of a new ePrivacy Regulation; however, it is too early to understand the implications on the industry of any changes under the ePrivacy Regulation.

## Brexit

While the impact of Brexit is currently uncertain, it is highly likely that the UK will continue to implement the GDPR in the short term and would need to maintain a law similar to the GDPR in the longer term. Statements from the UK ICO before and after the referendum have supported that view. Therefore, irrespective of whether or not your organisation has operations in other EU Member States (so that GDPR compliance would be required in any event), we recommend continuing with GDPR compliance projects as planned as it will come into force before the UK leaves the EU.

## Key Terms

| | |
|---|---|
| **data controller** | The organisation which alone or jointly with others **determines the purposes and means of the processing of personal data**. This definition is largely unchanged by the GDPR meaning that controllers still bear the primary responsibility for compliance. |
| **data processor** | The organisation which **processes personal data on behalf of the controller**. Again this definition is unchanged by the GDPR; however there are direct obligations on data processors for the first time (see below). |
| **personal data** | personal data is 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.<br><br>This is an incredibly broad definition and covers a very wide range of data and can include any of the following: name, email address, postal address, phone number, customer account numbers, place of work.<br><br>However, each of these data alone may not necessarily be personal data but, **when taken in combination with other data, if you are able to identify a natural person, the data will become personal data.**<br><br>Personal data is likely to include: traffic data, location data, call data records and IP addresses.<br><br>*It is important to remember that other laws may also apply to the retention and use of certain categories of data, e.g., rules in PECR in relation to traffic and location data.* |
| **Processing** | **Any operation or set of operations 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. |

# Key provisions in the GDPR

## Types of data and processing activities covered

The GDPR covers very similar categories of data and activities as the DPA. Broadly, it covers information relating to an identified or identifiable natural person. The new definition of personal data potentially broadens the scope of data covered and also specifically refers to identifiers such as an identification number, location data, an online identifier or to one or more factors specific to someone's physical, physiological, genetic, mental, economic, cultural or social identity. This means that a name is not necessarily required for information to be caught by the GDPR – any means of unique identification is likely to be sufficient.

Specific obligations apply to the use of:

- **special categories of personal data** - information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, along with genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation – this is what used to be known as "sensitive personal data";
- **profiling** - automated processing to evaluate, analyse and predict personal aspects, such as work performance, economic situation, health, behaviour, location; and
- **pseudonymisation** – processing data in a way such that it can no longer be attributed to a specific person without the use of additional information which is kept separately from it. (This is different to anonymisation, which in theory should not be reversible.)

# GDPR principles

While the requirement to make an annual notification to the ICO falls away for data controllers, there are plenty of other requirements to take its place as both controllers and processors become responsible for, and must be able to demonstrate, compliance with all of the principles relating to data processing. The principles in the GDPR are broadly similar but stricter than the existing eight principles in the DPA. They are:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation; and
- integrity and confidentiality.

Security and international data transfers are dealt with separately (see Practical Steps for Compliance Note).

# Legal basis for processing and consent

Where you are a data controller you must ensure that you have a legal basis to process the information, and not process data beyond the purposes for which it has been obtained. In most cases, you will be able to easily satisfy this requirement where data is required to perform a contract (e.g., a home address required to provide services) or to meet a legal requirement (e.g., obtaining the national insurance number of employees). See the Data Mapping section in the Practical Steps for Compliance for more detail on other lawful grounds for controlling and processing data.

### New processor obligations

For the first time processors will be directly responsible for compliance with data protection law, which is a significant change for those organisations acting as processors who up until now have only faced the obligations contractually flowed down to them by their customers who are controllers.

When acting as a processor, or passing data to a third party to process or sub-process on your behalf, the key new areas to consider and implement (where you are the controller) include a specific requirement:

- not to sub-contract their processing activities without controller consent or obtain consent to sub-processing;
- to maintain records of processing carried out on behalf of controllers, which must include: the name and contact details of processors, each controller and (where applicable) representative and DPO for each; categories of processing for each controller; transfers of data outside the EEA, including identification of the country; documentation of appropriate safeguards; a general description of technical and organisational security measures;
- to implement appropriate data security measures and notify controllers of security breaches;
- to appoint a DPO (where applicable); and
- to ensure that transfers of personal data out of the EEA are compliant.

## Who will the GDPR apply to?

You may be both a data controller and a data processor for different purposes in relation to different personal data and the GDPR will apply to both data processors and data controllers.

The GDPR also extends the territorial reach of the organisations that it applies to:

(a) EU organisations processing personal data in the context of their activities, regardless of whether the processing takes place in the EU; and

(b) organisations with no establishment in the EU who process personal data of EU based individuals where the processing relates to:

- the offering of goods or services to those individuals, whether or not payment is required; or
- the monitoring of their behaviour as far as their behaviour takes place within the EU.

The infographic below shows some situations where the location of your customer or the end user may affect whether GDPR applies. As you may not know the location/domicile of the end users it is best practice to ensure that your business complies with the GDPR for all customers.

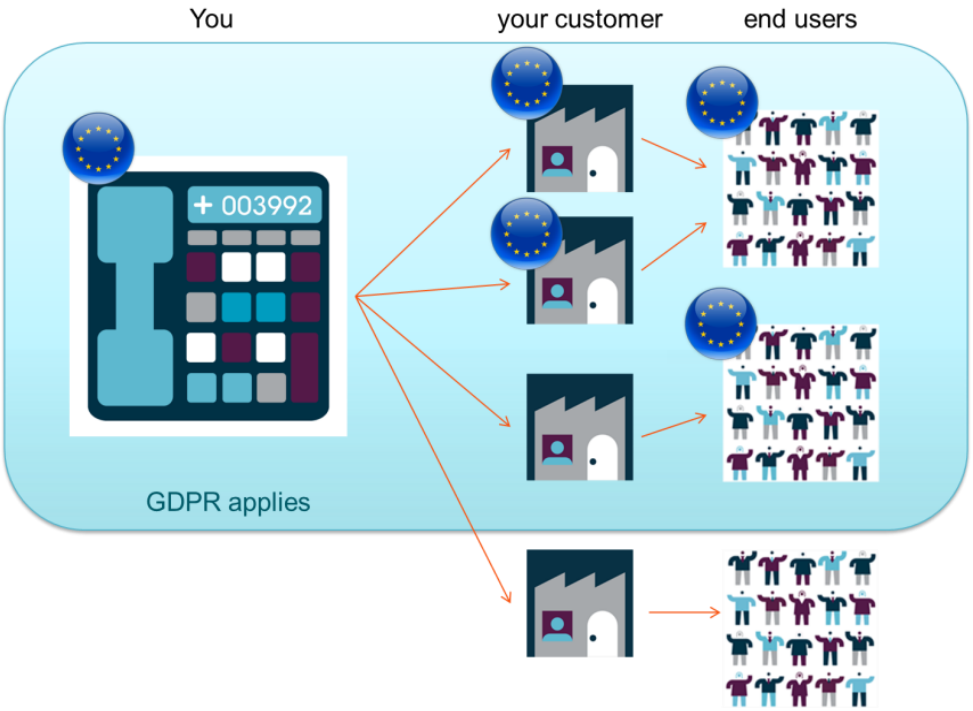
## Why Comply?

Non-compliance with the GDPR can result in fines of **up to 4% of global annual turnover or €20,000,000.** This is a significant increase on the maximum fine of £500,000 under the DPA**.** The types of breaches that could lead to fines of the highest level include: breaches relating to consent, rights exercised by data subjects and transfers outside the EEA. There is also a lower tier of fine for other breaches, e.g., breaches realting to the failure to implement technical and organisational measures to ensure data protection by design and default, of the higher of 2% of worldwide turnover or €10,000,000.

A failure by processors to meet their direct obligations under the GDPR may result in enforcement action by the ICO (or other relevant regulator) but a processor will only be liable where they do not follow the processor-specific obligations set out in the GDPR or the controller's lawful instructions.

In addition, data subjects will be able to bring claims for compensation against data controllers or data processors where they have suffered damage as a result of the other party's infringement of the GDPR.

There are also business benefits for compliance; it can be an opportunity to adopt a fresh approach to thinking about data privacy and protection and can be a way to build and enhance trust with your customers and employees.




## Practical Steps to Compliance

It will no longer be enough for you to be generally acting in a compliant way; you will also need to take steps to show that you are compliant. As a data controller you will be expected to implement appropriate technical and organisational measures to ensure and demonstrate compliance with the GDPR. In practice, this will mean using a combination of software tools, training, staff awareness and data protection policies.

The issues and suggestions below are designed to help you prepare a plan for your business as you work towards becoming GDPR compliant:

1. Create a planning roadmap for GDPR compliance
2. Data Mapping / conduct a privacy impact assessment
3. Assess Security measures
4. Review Breach Notification processes
5. Review and update your Contracts
6. Review and update your policies
7. Build awareness within your business
8. Appoint a Data Protection Officer
9. Review processes for responding to subject access requests
10. Include privacy considerations in new product/service development

11. Keep records

12. Review processes for international transfers of personal data

# 1 Planning Roadmap

Prepare a clear plan setting out the steps that you need to take to achieve GDPR compliance and assign clear roles, responsibilities, goals and actions to each step. This will help you track your compliance programme as we get closer to 25 May 2018.

# 2 Data Mapping

You should begin creating a "data map" of the personal data that your business controls and processes as part of a privacy impact assessment ("PIA"). A PIA is required before you begin processing activities, especially if they involve "new technologies" e.g., IoT and artificial intelligence, are likely to result in high risk to rights and freedoms such as automated processing (including profiling), or include large scale processing of "special categories" of data. We recommend you create a data map for all existing data processing activities to comply with this requirement.

Data protection authorities, including the ICO, are required to issue "white lists" and "black lists" of processing for which a PIA is or is not required.

These should help you to decide whether to carry out a PIA and whether to consult or not although they have not yet been published by the ICO. The ICO has a PIA Guide available on its website which it is in the process of updating: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

## Creating the data map

These should help you to decide whether to carry out a PIA and whether to consult or not although they have not yet been published by the ICO. The ICO has a PIA Guide available on its website which it is in the process of updating: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

Controllers will be expected to seek the views of data subjects or their representatives and in certain circumstances consult with the ICO (or other relevant data protection authority). Given the likely timescales involved in consulting with the ICO (up to eight weeks with a possible extension of six weeks or more if further information is required from a controller), controllers should approach any high risk processing with caution and ensure that substantial measures are in place to mitigate any risks so that no consultation with the ICO is needed. We await further guidance on the meaning of "high risk", which will be helpful in assessing when consultation may be required.

The data map should be a formal record (either hard-copy or electronic) of the personal data that your business controls. Not only is this a requirement for all data controllers under the GDPR but this will also prove invaluable to the business should you ever need to respond to an access request from an individual or a regulator or notify a regulator following a data security breach. The data map should include responses to the following questions from the relevant stakeholders within your business:

## 2.1 Where does personal data enter our business from? For example:

(a) New hires: Each time you hire a new employee, you will collect certain personal data about that individual (e.g., their name, address, bank account information, references from previous employers, etc.);

(b) Customer interactions: When dealing with customer queries and complaints, you may collect personal information in order to respond to their request (e.g., recordings of customer calls to your helpline); and

(c) Customer's data: If you receive personal data from your customers, which you then process on their behalf (e.g., OTT communications content or usage/consumption/location patterns).

### 2.2 Where does personal data leave our business? For example:

(a) Departing employees: Each time an employee leaves your business, you should only maintain copies of their records for a limited period of time. Do you also agree to provide them with copies of payslips/P60s?

(b) Outsourced service providers / Sub-processors: If you outsource your customer helpdesk function, than the service provider will most likely be acting as a data processor on your behalf. Similarly, if you use a third-party to host your servers (e.g., AWS) they will be acting as a data processor on your behalf; and

(c) Closing a customer's account: When a customer closes their account with you, will you delete or return their data (including all personal data)?

### 2.3 What personal data is captured at the points identified under 1 and what personal data is deleted or returned under 2?

You should identify the categories of personal data and data subjects in respect of each pool of data (e.g., Customer Data; names and contact details of customers or Employee Data; name, contact details, disability information).

### 2.4 Is any of the personal data processed by the business "special categories" of personal data?

Processing special categories of personal data will impose additional restrictions on businesses (e.g., you may need to apply higher levels of information security to such data). Special categories of data are: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health data, sexual orientation.

### 2.5 What "lawful ground" are you relying on in respect of each act of processing?

Each act of processing will need to have a "lawful ground" that justifies the processing by the business. The permitted "lawful grounds" are as follows:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes e.g., when user signs up to a specific service. The requirements for consent are set to be more difficult under the GDPR:

  (i) requests for consent must be clearly distinguishable from other matters, in an intelligible and easily accessible form and use clear and plain language;

  (ii) data subjects must be able to withdraw consent as easily as it was given and must be told upfront that this is possible;

  (iii) where contract performance is conditional on consent to processing personal data that is not necessary for performance of that contract, such consent is unlikely to be "freely given" – you will need something more in these situations or must be able to rely on one of the other lawful grounds for processing; and

  (iv) controllers must keep clear evidence of consents obtained.

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the data controller is subject, e.g., data retention obligations under the Investigatory Powers Act 2016 or call recording obligations under MIFID II (for investment firms);

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

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

(f) processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Legitimate interests could include processing to prevent fraud, for direct marketing purposes, internal administrative purposes within a group, and ensuring network and information security. Controllers will need to make a careful assessment in each case, including by taking account of the reasonable expectations and legitimate interests of the data subject.

## 2.6 Where is personal data stored?

Businesses should know the location of the personal data that they store, ideally this should identify which server each pool of data is stored on, whether the server is owned by the company or a third party and the geographical location of that server. For real-time communications (where no call recording solution is in place) you may not be storing the personal data that is processed as it is only processed whilst in transit – this data should be still be included on your data map.

## 2.7 Where is personal data transferred?

(a) Within the EU: Agreements for the processing of personal data by data processors on behalf of data controllers are required to contain certain provisions, as specified under the GDPR. Failure to include such provisions will place the parties in breach of the GDPR and expose them to potential fines. These are discussed in more detail in the Practical Steps for Compliance.

(b) Outside of the EEA: Is personal data ever transferred outside of the EEA? For example, do you outsource your help desk function to India? If so, this will classify as a transfer of personal data to a country outside of the EEA. Different obligations will apply in respect of where the personal data is transferred to, as follows:

(i) Transfers to the U.S.A: Transfers to the U.S.A are not permitted unless:

- The recipient is certified under the U.S Privacy Shield; or
- The parties have agreed model contract clauses;

(ii) Transfers to Permitted Territories: Transfers to the following countries do not require any additional protections beyond those required for transfers within the EEA: Andorra, Argentina, Canada, Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand and Uruguay.

## 2.8 What security measures are applied to personal data?

(a) Businesses are required to apply "appropriate technical and organisational standards" to the personal data that they process. It is down to the business itself (in consultation with its information security team or advisors) to determine if the security measures it applies are adequate to protect the data in question. This should be an on-going assessment as the state of the art develops.

(b) Is different personal data protected in different ways? Higher risk data will require a greater level of information security. For example, businesses should consider applying a higher standard of IT security to "special categories of data" for example ensuring this data is encrypted.

## 3 Security Measures

For the first time, there are security measures specifically covered in the GDPR and you will need to review your current security measures/policies to ensure that they meet the new requirements, such as:

- pseudonymisation and encryption of personal data;
- the ability to ensure on-going confidentiality, integrity, availability and resilience of systems and services processing personal data;
- the ability to restore the availability and access to data in a timely manner in the event of an incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring security of processing.

You are required to evaluate the risks inherent in the processing that you are conducting and implement measures to mitigate those risks.

Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. Any measures you put in place should be considered alongside the Ofcom Security Guidelines https://www.ofcom.org.uk/__data/assets/pdf_file/0021/51474/ofcom-guidance.pdf

### Assessing Data Security Risk

In assessing data security risk, consideration should be given to the risks that are presented by processing personal data, such as:

- accidental or unlawful destruction;
- loss or alteration; and
- unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

## 4 Breach Notification Processes

The GDPR brings in new breach notification requirements for notifications of personal data breaches to:

- the regulator; and
- the data subjects.

These notification obligations are in addition to those security / network breach notification obligations in PECR and set out in the Ofcom Security Guidelines https://www.ofcom.org.uk/__data/assets/pdf_file/0021/51474/ofcom-guidance.pdf which may not have caused a personal data breach triggering notification obligations under the GDPR.

You should be reviewing your existing policies and processes for breach notification to ensure they meet the GDPR requirements. It is also recommended to test these processes – you don't want to be

using a new internal breach notification process for the first time when you have suffered a real data breach.

### Breach notification to regulators

Controllers must report "*personal data breaches*" to the ICO (or other relevant data protection authority) without undue delay and, where feasible, within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in risk for the rights and freedoms of individuals. It is difficult to imagine many situations where a data breach wouldn't result in this risk and therefore if you rely on this exception you should have strong reasons why. This threshold/policy should be reviewed periodically to ensure the risk profile has not changed.

A personal data breach is defined quite widely to include: "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*". A number of different types of incident could therefore trigger a requirement to notify.

The notification itself must include various information, such as, a description of the nature of the breach, the categories of data and number of people involved and approximate number of records. Both the effect and remedial action taken by the controller must be provided. Whilst this information may be provided in phases, it nonetheless highlights the importance of good incident management policies and processes, not least so that you can make an informed decision about whether to notify and how this should be managed effectively.

### Breach notification to data subjects

The GDPR also introduces a new requirement to notify affected individuals without undue delay if their rights and freedoms are put at high risk. The notification must describe the nature of the breach in clear and plain language and also include details of the DPO (or other contact point), the likely consequences, and the measures being taken to address the breach.

There is an important exception to the requirement to notify if one of certain conditions has been met:

- the controller has implemented measures to protect the data, including those that render the data unintelligible, for example, encryption;
- the controller has taken measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; or
- notifying data subjects would involve disproportionate effort, although in such circumstances a public communication is then envisaged.

The ICO (or other supervisory authority) may also require a controller to notify data subjects even if the controller had previously decided not to notify them.

## 5 Review and update your Contracts

A data controller must ensure that it has in place a contract with a third party data processor. Before appointing a data processor (or sub-processor) you should also ensure that you have conducted sufficient due diligence to ensure that the GDPR requirements will be met and the rights of data subjects will be protected. This obligation also applies to data processors.

The GDPR sets out much more prescriptive requirements for a binding contract between the controller and processor than the DPA.

We recommend that you review your supplier and customer contracts to assess if data processing is in-scope of that relationship and undertake a review of the contract to ensure it complies with the GDPR requirements.

## Review of customer and supplier contracts

We recommend that you review your supplier and customer contracts to assess if data processing is in-scope of that relationship. Where it is:

- you should review if your supplier contracts e.g., outsourced contact centre, cloud hosting provider, or your customer contracts, where you are processing personal data on behalf of your customers when providing your services, include sufficient clauses to meet the GDPR requirements. GDPR clauses can be included in your main customer agreement or in a separate data processing agreement; and
- prepare variations to such contracts to reflect the GDPR requirements that will continue in force after 25 May 2018.

Whilst this requirement applies to the data controller you may wish to approach your customers to update your standard terms to manage the workflow of such variations and maintain, insofar as possible, standard terms with your customers.

The contract itself must also include specific provisions (see the Checklist), which could in due course be covered by standard contractual clauses (similar to those used for data transfers) laid down by the European Commission.

## Contracts Requirements Checklist

Contracts must include:

- the subject matter and duration of processing;
- the nature and purpose of processing;
- type of personal data;
- the categories of data subjects; and
- the obligations and rights of the controller.

The contract must specify that the processor:

- follows the controller's instructions (including regarding data transfers outside the EEA);
- imposes confidentiality obligations on persons handling data;
- ensures the security of processing (as described above);
- notifies the controller of any personal data breaches;
- does not engage sub-processors without the controller's consent and a written contract flowing down the same obligations;
- assists the controller in responding to requests from data subjects;
- assists with consultations with supervisory authorities;
- allows the controller to decide whether data should be deleted or returned on termination of the contract;
- supports the controller by providing evidence of compliance and audits; and
- notifies the controller if any of their instructions breach the GDPR or UK data protection law provisions.

## 6 Review and update your policies

Transparency is a key theme of the GDPR and so the format, positioning, provision and content of privacy notices/policies takes on new significance, especially where consent from data subjects is required before data processing can begin.

As a minimum businesses should have the following policies in place in order to raise awareness internally and in order to be as transparent with customers as possible (as is required under the GDPR):

**External Privacy Policy:** If your business collects personal data directly from data subjects, you should have an externally facing privacy policy that explains to the data subjects:

- who you are (including contact details) and that you are acting as the data controller;
- what personal data you collect from them;
- how you use the personal data that you collect;
- who (if anyone) you share their personal data with;
- if you transfer their data cross-border;
- how long you store their personal data for (or relevant criteria for determining this);
- how they can exercise their rights under the GDPR or raise complaints against you; and
- if you have a Data Protection Officer, who they are and how they can be contacted.

Privacy notices must be concise, transparent, intelligible and in an easily accessible form. They must also be drafted using clear and plain language.

These requirements must also be met if you do not obtain information directly from the data subject. This leads to potential challenges it you rely heavily on information gathered by third parties.

**Internal Privacy Policy:** You must inform your employees about how you process the personal data that you collect about them during the course of their employment, this should include the same information as you include in the external privacy policy.

Further information on privacy policies can be found under the ICO's 'Privacy Notices Code of Practice' found at https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

## 7 Build awareness within your business

A key element of compliance under the GDPR is building awareness about the importance of data protection and the measures that businesses should take not only to prepare for the GDPR but how to adjust to the new processes (e.g., data breach responses) that will be in place after the GDPR comes into force.

The most effective way for business to raise awareness is:

- through training employees in the run-up to the GDPR coming into fore and to schedule regular on-going data protection training; and
- to update your internal policies to address the additional rights of data subjects and additional obligations on the business under the GDPR.

## 8 Appoint a Data Protection Officer

You must appoint a data protection officer ("DPO") if your business:

(a) carries out regular and systematic monitoring of individuals on a large scale; or

(b) carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions.

We are expecting further guidance on the application of these terms and the meaning of "large scale". In other cases, a DPO is optional unless required by EU and/or local law and we recommend appointing someone within your business to take primary responsibility and main point of contact for data protection compliance.

### Choosing a DPO

When appointing a DPO you should consider the following:

DPO should have a degree of independence to enable them to carry out their role without instruction and be able to report directly to senior management;

- DPO should have the knowledge, support and authority to carry out their role effectively (a DPO is expected to have expert knowledge of data protection law and practice to monitor compliance and provide advice internally);
- the DPO could be an employee or an external contractor such as a consultant or law firm;
- any other day-to-day activities that the DPO undertakes for you should not conflict with the role of DPO;
- the DPO cannot be dismissed or penalised for performing their tasks; and
- it will be possible for a group of undertakings to appoint a single DPO but they must be easily accessible from each company. So, for companies with multiple offices across different time zones and/or locations, more than one DPO may be needed.

## 9 Review processes for responding to subject access requests

One of the key changes under the GDPR is the increase in the explicit rights of the data subjects. You should check your procedures to ensure they cover all the rights individuals have. This will include assessing how you would delete personal data or provide data electronically and in a commonly used format

### Rights of Individual

The GDPR includes the following rights for individuals:

- the right to be informed. This includes being told the source of the information and where it was not collected directly from them;
- the right of access. See more detail below;
- the right to rectification. Inaccuracies should be corrected without undue delay;
- the right to erasure aka 'the right to be forgotten'. A data subject can request that their information is deleted where it is no longer necessary in relation to purposes for which it was collected, or they withdraw consent (and no other ground for processing applies), or the processing is unlawful. If data has been made public by a controller, then they must delete it as far as possible taking into account available technology and costs. Requests must be satisfied without undue delay. There are, however, some potentially useful derogations that may apply, such as where a controller would need to retain information to comply with legal obligations, such as employee tax records;

- the right to restrict processing;
- the right to data portability. Data subjects will have the right to request that their data is moved to another controller (i.e., a new service provider) in a structured, commonly used and machine-readable format if technically feasible;
- the right to object to processing which a controller was carrying out based on the controller's legitimate interests, such as direct marketing or profiling, or where decisions were being made based solely on automated processing including profiling; and
- the right not to be subject to automated decision-making including profiling.

Other than the 'right of access' (see below), we do not discuss these rights in detail under this note, however, further guidance can be found about data subjects' rights on the ICO website.

### The Right of Access

You should have processes in place to deal with data subject access requests (i.e., where a data subject asks you to provide them with confirmation of whether or not you process their personal data and, if you do, with information about the processing that you perform).

In respect of data subject access requests:

- in most cases you will not be able to charge for complying with a data subject's access request;
- you will have a month to comply;
- you can refuse or charge for requests that are manifestly unfounded or excessive; and
- if you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.

## 10 Privacy by design and default

The GDPR emphasises the concept that data protection should not be an afterthought or an issue casually considered at the end of a project or bolted on to procedures; it must be central to the way that organisations plan and operate. Systems and processes must be designed with data protection compliance in mind and must by default ensure that only data necessary for each specific purpose is processed and that it is not accessible to an indefinite number of individuals.

Throughout a product/service lifetime and when developing new products/services you should consider using measures (such as pseudonymisation and data minimisation) designed to implement data protection principles think about appropriate organisational and technical measures.

## 11 Keep records

Where you are a data controller you must maintain written records of your processing activities, except in certain limited circumstances, and must make these available to supervisory authorities on request. Where you are a processor, controllers are likely to flow down this requirement contractually and it is therefore advisable to keep records about all data processing activities undertaken.

The records should include:

- the name and contact details of processors, each controller and (where applicable) representative and data protection officer;
- purposes and categories of processing;

- categories of data subjects;
- categories of recipients of personal data including overseas;
- details of transfers outside the EEA, including documentation of appropriate safeguards;
- data retention periods; and
- a general description of technical and organisational security measures.

## 12 International data transfers

The existing cross-border transfer rules and derogations remain largely unchanged, in that in order to transfer data outside of the EEA, one of a number of solutions must be in place. These include: data subject consent; a finding of adequacy in respect of the recipient country; standard/model contractual clauses; binding corporate rules; or that the transfer is required for the performance of a contract.

If a controller wants to use non-standard contractual clauses, they will need to obtain approval from the ICO or another appropriate data protection authority. In addition, if data subject consent is relied upon, it must be explicit and the individual must have been informed of the risks – again this emphasises the focus on transparency.

There is a potentially useful new "derogation" where other standard derogations cannot be used, if the transfer is: not repetitive, concerns only a limited number of individuals, is necessary for the purposes of compelling legitimate interests of the controller and where this is not overridden by the interests, rights or freedoms of the data subjects involved. The controller must also have assessed all the circumstances, adduced suitable safeguards, informed its data protection authority and notified the data subjects of the transfer and the "compelling legitimate interest" of the controller.

## Contacts

**Hannah Drew (née Willson)**
**Associate Director**
T: +44 20 7105 7184
Hannah.drew@osborneclarke.com

**ITSPA Secretariat**
T: 020 3397 3312
team@itspa.org.uk

**Nina Cummins**
**Partner**
T: +44 20 7105 7158
nina.cummins@osborneclarke.com

**Jon Fell**
**Partner**
T: +44 20 7105 7158
jon.fell@osborneclarke.com

**Mark Taylor**
**Partner**
T: +44 20 7105 7640
mark.taylor@osborneclarke.com