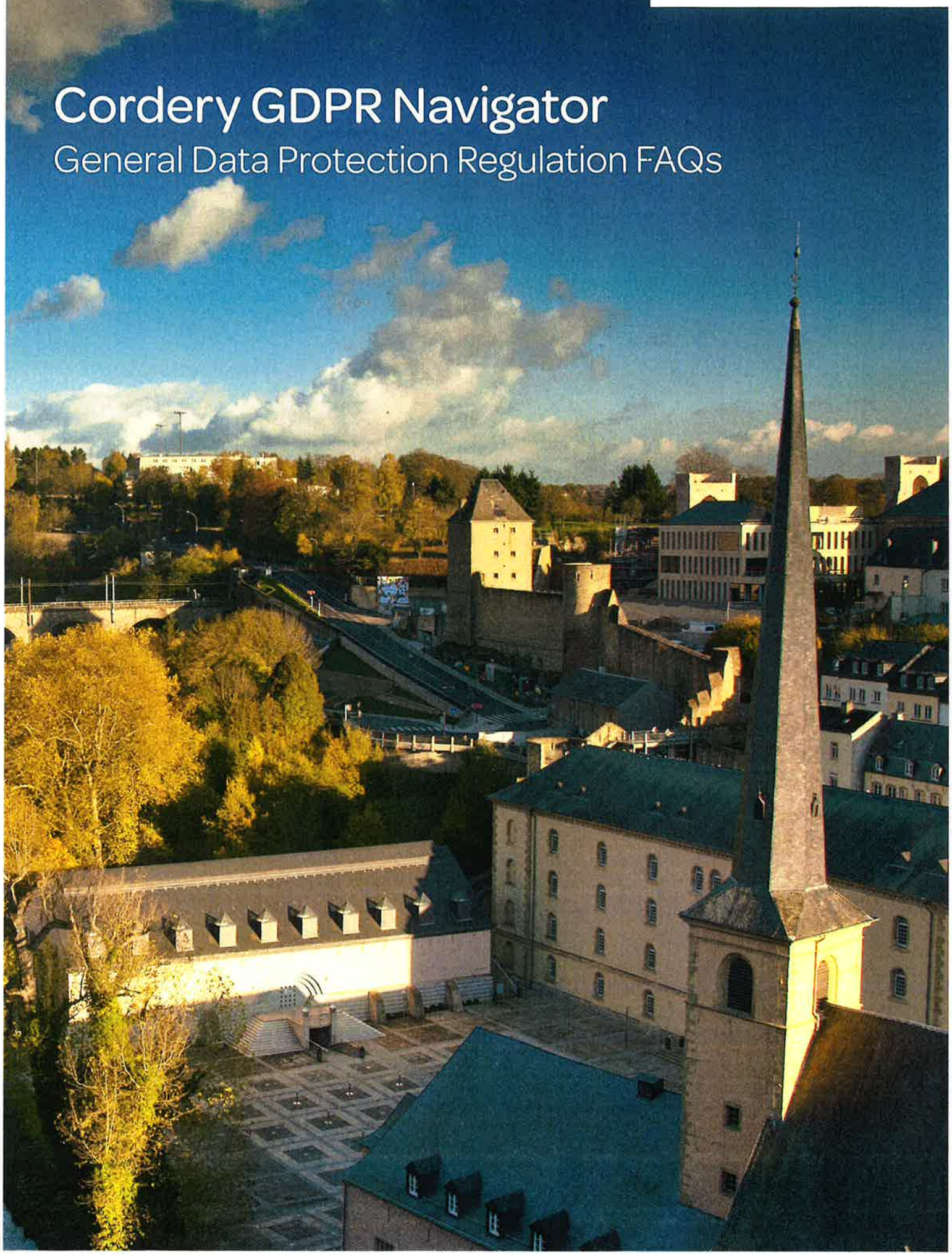
Cordery
Legal.Compliance

Cordery GDPR Navigator

General Data Protection Regulation FAQs



This note is part of Cordery GDPR Navigator. You can find out more about GDPR Navigator by visiting www.bit.ly/gdprnav. Technical terms are used in this document which are explained in the Cordery GDPR Navigator glossary.

What is this all about and where do things stand now?

The EU has now changed its data protection rules. From 25 May 2018, the General Data Protection Regulation (or GDPR) applies.

These changes go well beyond an upgrade. For all businesses, GDPR has meant some level of change to processes, policies and operations.

Everyone who handles personal data is likely to need an understanding of what GDPR is about. These FAQs aim to help with that process.

Further reading:

See GDPR Articles Index in GDPR Navigator for a full list of the provisions in GDPR.

What is EU data protection?

In the EU personal data can only be processed under strict conditions and for legitimate purposes only – those who collect and manage personal information must protect it from misuse and must respect data protection rights. Personal data has a wide definition under GDPR – it could include for example IP addresses and device identifiers. You can find out more about personal data in the glossary.

Data protection was previously regulated in the EU under a 1995 Directive that controlled the processing of personal data. EU Member States had to implement this Directive into their own national law. Some countries had their own data protection laws prior to the 1995 Directive and there were differences in the way that the Directive was implemented across Europe. These data protection laws were of very wide effect with major compliance requirements placed on businesses inside and outside the EU. However, this disjointed approach to data protection law created an unreasonable compliance burden for businesses operating across different EU Member States and was a barrier to effective cross-border trade.

Why the change?

The data world of 1995 was significantly different to today and so it was felt that a significant overhaul was needed in order to make it fit for purpose for the digital age and properly protect the rights of individuals. Key aims of these changes include having:

- a uniform regime;
- a less administratively burdensome and costly regime for businesses;
- an extension and expansion of rights; and,
- making privacy by design the norm.

Are these completely new rules?

Yes and no. Yes, the 1995 rules have been completely replaced. No, not only will the fundamental aspects of privacy continue to be protected, they have also been extended. The changes essentially build on the previous structure whilst also introducing many new elements.

What are the main changes?

The new rules are in the form of a Regulation (as opposed to a Directive). EU Regulations require no further legislation to be adopted by EU Member States to make GDPR the law in their national systems. This means that (in principle at least) the EU data protection rules should be the same in all 28 EU Member States.

This said, GDPR allows some latitude for EU Member States to adopt their own additional rules in some areas, for example to be more specific about the processing of employees' data for the purposes of recruitment. It also allows for additional law in unaddressed areas, including processing data about deceased persons. In addition, Member States like the UK have passed local laws to preserve existing aspects of their national data protection rules that are additional to the rules set out in GDPR.

So, the general approach that we have seen to date is that each EU Member State has:

1. the 'core' data protection rules set out in GDPR; plus
2. some additional local law.

Whilst the main focus for businesses will be the core rules, which will be largely the same throughout the EU, to ensure full compliance businesses will still need to check for any local variances.

Further reading:

See GDPR Navigator Quick introduction to the Regulation video briefing.

Our business is not in the EU so will these rules still affect us?

Potentially. GDPR will apply not only to businesses which are actually established in an EU Member State, but, also, to businesses outside the EU that either process the personal data of individuals in the EU to:

- offer them goods and services (whether paid for or not); or
- monitor their behaviour where their behaviour takes place within the EU.

GDPR says that the mere accessibility of a business' website in the EU or of an email address and of other contact details or the use of a language generally used in the country outside the EU where the business is established is not enough to bring a business under GDPR. But, GDPR also states that factors such as:

1. the use of a language or a currency generally used in one or more EU Member States with the possibility of ordering goods and services in that other language, and/or
2. mentioning customers or users who are in the EU,

may be factors to indicate that a business envisages offering goods or services to individuals in the EU, which would bring the business within the scope of GDPR.

For a business that is a data controller or data processor located outside the EU which comes within the territorial scope of GDPR, this may mean having to designate (in writing) a representative in the EU. This data protection representative is known as a DPR. The DPR rules do not apply to all organisations – those that only carry out occasional data processing that does not involve large-scale processing of more sensitive categories of personal data and is unlikely to result in a high risk to individuals' rights are exempt.

This extra-territorial dimension is a real change, and has increased the number of non-EU businesses that come within the scope of EU data protection law. However, this is intended to ensure that the rights of individuals whose personal data is processed in a significant way by an organisation are protected, irrespective of where that organisation is based.

Further reading:

See Geographical Reach in GDPR Navigator.

How many data protection regulators will we have to deal with?

Under GDPR national independent regulators remain in place. There will not be a single centralised EU regulator. A key aspect of GDPR is that a business (referred to as an "establishment" under GDPR) should only have to deal with one data protection authority (DPA). This system is known as the One-Stop-Shop system. Technically, DPAs are called a "supervisory authority" under GDPR, but the concept is similar to that of a DPA under the old law.

To enable a business to deal with just one DPA, under GDPR, the DPA of either the main establishment, or, (if this is the case) of the single establishment of a data controller or data processor, will act as lead supervisory authority in situations where data processing carried out by that data controller or data processor is cross-border – i.e. it cuts across EU Member States. A particular EU co-operation procedure between DPAs will apply in these cases – the lead DPA will work closely with the other DPAs on the matter in question.

There's quite a complicated system in place to work out who the lead DPA will be. This is not something that an organisation can select for themselves.

The European Data Protection Board (EDPB), which replaces the previous Article 29 Working Party (an important grouping of EU data protection regulators) will get involved in difficult cases. The EDPB has as one of its functions the role of dispute resolution in disputes between DPAs, notably between the lead supervisory authority and other DPAs.

So, businesses may only have to deal with one DPA but this DPA may well be interfacing with other DPAs. This One-Stop-Shop approach is a welcome step forward in terms of simplifying compliance and ensuring consistent application of GDPR by DPAs, but, because of its nature the co-operation procedure may also lead to administrative and bureaucratic delays for businesses.

Will we have to register with a DPA?

Potentially – although in a different way to pre-GDPR days. Previously there were requirements in some countries for a data controller to register with or "notify" their data processing activities to a DPA and pay a registration fee. This process will largely disappear, as will the registration fee as a source of revenue for the DPA. Each DPA is dealing with this in different ways – in the UK, for example, there will be:

- a new data protection fee for data controllers to pay based on their size; and
- a new register of fee payers, including information such as data controller contact details and data protection officer (DPO) details.

The amount information that will need to be filed with the DPA will reduce. But, just as one regulatory obligation lessens another one takes its place!

Both data controllers and data processors need to maintain records of their data processing activities. Those records must contain some mandatory information (which may be more detailed than that required under the previous registration process). These records will need to be made available to the DPA for inspection on request.

Also, where new data protection impact assessment (DPIA) process applies (see below) a DPA must be consulted (with the submission of information) prior to the processing of personal data where an assessment indicates that the processing would result in a high risk in the absence of measures taken by a data controller to mitigate the risk.

Further reading:

See One-Stop-Shop, the Powers of a DPA and the Role of the EDPB in GDPR Navigator.

Further reading:

See One-Stop-Shop, the Powers of a DPA and the Role of the EDPB in GDPR Navigator.

What are special categories of data?

Special categories of data are similar to sensitive personal data under the old law. GDPR defines Special Categories of Personal Data as follows:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- the processing of 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.

Special precautions must be taken with these types of data. Data relating to criminal convictions and offences has special treatment under GDPR too.

Will data controllers and data processors have more to do?

Yes, data controllers and data processors will have considerably more responsibilities and obligations under GDPR. Data processors will now have direct obligations, and, exposure to fines under GDPR.

Some of the key obligations include:

- Technical and organisational measures – a data controller must implement technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with GDPR, including the implementation of data protection policies.
- Data processing records – as mentioned above, data controllers and data processors will have to maintain records of processing activities, according to detailed criteria set out under GDPR, which must be made available to DPAs on request.
- Data processor contracts – GDPR also stipulates that processing by a data processor on behalf of a data controller must be set out in a contract that contains mandatory provisions. Data processors have far more responsibilities under GDPR and as a result it will often be in their best interests to make sure that they get the contract right as well.

An important practical result is that the documentation of data processing activities and responsibilities will need to be undertaken more fully by businesses, and, due diligence on suppliers and data processing provisions in contracts will have to be done more rigorously.

Further reading:

See Data Controller or Data Processor - What do these Terms mean and Which are You, Appointing Data Processors – How to Reduce your Risk and The Security Provisions of GDPR in GDPR Navigator.

Will we have to make privacy an integral compliance element in our business?

Yes. Privacy by design and/or privacy by default will not be an add-on, but, instead, becomes the norm as businesses have to incorporate data protection safeguards into their products, services and processes right from the start.

Organisations have to implement appropriate technical and organisational measures for data processing, such as anonymisation or pseudonymisation (the processing of personal data in such a manner that the personal data can no longer be attributed to a specific individual without the use of additional information), in order to implement data protection principles such as data minimisation.

Data controllers have to implement appropriate measures to ensure that, by default, only personal data which are

necessary for each specific purpose of the processing are processed – this will include the amount of personal data collected, the extent of their processing, the period of their storage, and, their accessibility. The measures must also ensure that by default personal data is not made accessible without an individual's intervention to an indefinite number of people.

Data security is also a key element of any data protection compliance programme. GDPR is more prescriptive about the security measures that need to be considered – this includes encryption and regular security testing.

GDPR summarises some of these responsibilities in 6 Data Protection Principles which are at the heart of good data processing. We've summarised the main points in each Principle below but you can find more detail in GDPR Article 5.

The Data Protection Principles deal with:

a. Lawfulness, fairness and transparency – make sure that data is processed lawfully, fairly and transparently;

b. Purpose limitation – make sure you only collect data for specified, explicit and legitimate purposes. Don't process data in a way that is incompatible with those purposes;

c. Data minimisation – make sure your use of data is adequate, relevant and limited to what is necessary in relation to the purposes for which you process data;

d. Accuracy – make sure your data is accurate and, where necessary, kept up to date;

e. Storage limitation – don't keep data for longer than necessary;

f. Integrity and confidentiality – make sure data is processed in a manner that ensures the appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Make sure you use appropriate technical or organisational measures.

Bear in mind that some people, including the UK DPA, the Information Commissioner's Office (ICO), add a seventh principle – known as the accountability principle - which comes from GDPR Article 5(2) saying:

"A data controller shall be responsible for and be able to demonstrate compliance with the six principles."

The practical application of these measures requires time and effort on the part of a business to implement. In addition product development teams and those who develop and design systems and processes that involve personal data processing need to keep on top of these requirements.

Further reading:

See The Security Provisions of GDPR in GDPR Navigator and our Information Security and its critical role video briefing.

Will consent be required for data processing?

Potentially. Consent is one of a number of available legal bases that can be relied on by a data controller to legitimise its data processing activities. Using consent as the basis of data processing is best suited to situations where an individual has a genuine choice as to whether their information will be processed in the way requested by the data controller. If you intend to go ahead and process the data anyway (even if the individual withdraws their consent), an alternative legal basis will generally be more appropriate. There are some circumstances (such as in an employment relationship) where consent will only be appropriate in exceptional cases – this is because the imbalance of power means it will be difficult to show that consent was *"freely given"*.

Under GDPR, the requirements for consent have also been recalibrated and the standard for valid consent is much higher. The GDPR definition is that consent means *"any freely given, specific, informed and unambiguous*

indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Businesses cannot rely on silence or opt-outs and instead an active consent process such as (clear) tick boxes is required. According to GDPR *"Silence, pre-ticked boxes or inactivity should not therefore constitute consent".* Businesses must also be able to demonstrate that consent has actually been given by individuals to the processing of their personal data, which means more recordkeeping obligations.

GDPR also has special rules for the offer of online services directly to a child. The processing of a child's personal data is only lawful where the child is at least 16 years old. Where the child is below 16 processing is lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Some EU Member States have set a lower age for these purposes, but this cannot be below 13 years old. Data controllers must make reasonable efforts to verify in these cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

Additionally, one of the available conditions that can be relied on to process sensitive personal data (or special categories of personal data) is "explicit consent". The main difference as compared to normal consent is that this requires a clear statement in words (as opposed to by an action or implied consent).

Consent is a requirement that businesses therefore have to pay special attention to – in some ways, for many types of data processing, it should be treated as the legal basis of last resort. If consent is used as the basis of processing, businesses will need to make sure that they can meet the raised bar for valid consent. They will also need to make sure that they have a mechanism in place to deal with any withdrawal of consent.

Further reading:

See Consent in GDPR Navigator and our Consent video briefing.

Are there any new rights for individuals (data subjects)?

Yes. Some new rights have been introduced and some of the previous rights have been expanded.

There is the "Right to Portability", which is an individual's *"right to receive the personal data concerning him or her, which he or she has provided to a data controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided".*

There are also rights not to be subject to some types of automated decision-making and profiling. Here "profiling" is defined as *"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a person, in particular to analyse or aspects concerning a person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".* The right is technically called the "Right to Object" as it is a right to object to being profiled, and, where personal data is processed for direct marketing that can also be objected to including where profiling is used for direct marketing. For direct marketing-related profiling, if an objection is received, all such profiling must stop (without exception).

GDPR also created a statutory Right To Be Forgotten (also called the Right to Erasure), which is the right to have personal data erased "without undue delay", based on certain grounds, for example where data is no longer necessary in relation to the purposes for which they were collected or otherwise processed. This sets out in law the Right To Be Forgotten that was previously the subject of a number of cases, including in the European Court's 2014 ruling in the Google case, which we have written about at

http://www.corderycompliance.com/european-court-google-ruling/. Right To Be Forgotten applications have also been made in other jurisdictions, for example, in France there have already been attempts to extend the European Court's ruling.

There may be some challenges in implementing these rights, although it should also be emphasised that all these rights are qualified, i.e. they are not absolute and have their limits and exceptions.

It should also be noted that under GDPR there are some changes to Subject Access Requests (SARs). A SAR is the process by which someone can exercise their right to gain access to the data held on them. SARs (along with most other data subject requests) must usually be answered within one month of receipt of the request. This can be extended for a maximum of two further months when necessary taking into account the complexity of the request and the number of requests. If an organisation wants an extension it must tell the data subject before the one month initial time limit has expired. Additionally, the ability for a business to ask for a fee for a SAR has been abolished (although some administrative costs may be recoverable in certain limited circumstances).

Some organisations have experienced a significant rise in the number of SARs they have received in the period since GDPR went live. We expect this was due in particular to SARs being free but also due to individuals having increased awareness of their rights. Given the prevalence of email, CCTV and cloud applications in particular, SARs are also now more costly and complex to deal with. That complexity is illustrated by a UK High Court case on SARs in 2016 which we have reported on at http://www.corderycompliance.com/subject-access-requests-and-investigations/.

An essential part of any organisation's data protection strategy is putting proper processes in place to deal with SARs. This requires not only internal processes and training but may also involve self-service mechanisms for data subjects, for example, through a business' website if they receive high volumes of requests.

Further reading:

See the Right to Data Portability, Subject Access Request and Right to be Forgotten Procedure and Subject Access Request Policy in GDPR Navigator and our video briefings on Right to be forgotten, Right to portability and Profiling / Automated Decisions.

Will we need to appoint a data protection officer?

Possibly. A Data Protection Officer (DPO) will have to be appointed to deal with data protection compliance where the core activities of the data controller or the data processor consist of:

- processing operations which, by virtue of their nature, scope and/or purposes, require regular and systematic monitoring of data subjects on a large scale; or
- processing on a large scale of special categories of personal data (outlined above) or, data relating to criminal convictions and offences.

There is regulatory guidance available that helps organisations to assess whether processing is "core", "regular and systematic" or "large-scale" (as the case may be). It is important to remember, however, that as with all guidance, guidance is just guidance. Ultimately questions of law will be for the courts to decide.

The DPO must be suitably qualified and is mandated with a number of tasks, including advising on data-processing, and, must be independent in the performance of their tasks – they should report directly to the highest level of management.

Businesses will therefore have to determine whether a DPO must be appointed or not. However, given the significance of privacy compliance today, even if technically-speaking a DPO is not required, a business of a particular size that regularly processes data would at least need to appoint

a suitably qualified person to be responsible for data protection compliance.

Further reading:

See DPO Job Description and Role Profile in GDPR Navigator and our Being a Data Protection Officer video briefing.

When will we have to report data breaches?

Ensuring that data is secure is one of the backbones of GDPR. Significant changes concerning the mandatory reporting of data breaches have been introduced requiring reporting to a DPA in most cases and, in many cases, communication to those affected in addition.

In this context a personal data breach means *"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"*. This covers many types of situations.

Most breaches will have to be reported, under conditions set out in GDPR including what action has been taken to mitigate them, to the relevant DPA without delay and, *"where feasible"*, not later than 72 hours after a data controller has become aware of the breach – a reasoned justification must be provided where reporting is not made within the 72-hour period.

There is however an important caveat to the breach reporting obligation as it will not apply where *"the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals"*. It will be for businesses to make this call on a case-by-case basis. However, the threshold is low and would cover any risk that is not remote.

Data processors are required to notify the data controller of all personal data breaches *"without undue delay after becoming aware"* of the breach.

Communication of a breach to the data subject(s) concerned must also be carried out when the *"breach is likely to result in a high risk for the rights and freedoms of individuals"*. If this is the case, the breach must notified to those affected without "undue delay" (i.e. no time-limit as such has been set). Caveats to this obligatory communication also exist, for example where the data affected by the breach has been encrypted. Data breach reporting is made more complicated still by:

- the fact that some countries (including Austria, Germany and the Netherlands) already had their own data breach reporting obligations;
- data breach reporting may be required under other rules and regulations, particularly in the financial and health sectors; and
- additional separate legislation is being implemented across the EU.

Businesses must therefore put in place a clear data breach action-plan and policy as a top priority and train staff accordingly.

Further reading:

See Data Breach Log, Data Breach Procedure and Data Breach Report Form in GDPR Navigator and our Dealing with a Data Breach video briefing.

What about liability and compensation?

As a general principle, any person who has suffered "material or non-material damage" (i.e. both financial losses and other damage, such as emotional distress) due to an infringement of GDPR has a right to compensation from the data controller or data processor concerned for the damage suffered – defences to liability are also set out under GDPR.

Generally, the issue of liability for data protection infringements is a growing topic. We have

already seen lots of activity in this area.

Because of the extra risk that a data infringement may now entail under GDPR, especially a data breach, businesses will need to do the maximum to minimise the potential for damages claims.

Will there be mandatory audits and dawn raids?

Yes. Under GDPR DPAs may *"carry out investigations in the form of data protection audits"*, and they may *"obtain access to any premises of the data controller and the data processor, including to any data processing equipment and means"* in line with relevant procedural law (obtaining a warrant etc.). This may prove to be a significant tool in a DPA's armoury. Businesses therefore need to put in place procedures and train staff to deal with this.

It is important to remember that DPAs also get significant additional powers under GDPR – for example the power to request information, to order a DPIA and to suspend processing. In some cases the exercise of these powers could be more damaging than a fine.

What kind of fines can our business face for breaching the rules?

Under GDPR, DPAs have the power to impose high fines for infringing GDPR. Different bands of fines will be applied in relation to three different sets of categories of infringement. Different bands of fines apply in relation to three different sets of categories. The highest level of fine is either a maximum of €20 million or 4% of the global annual turnover of a business, whichever is the greater, which will apply to the most serious infringements. DPAs will consider aggravating and mitigating factors - the approach that will be taken is very much on the lines of EU competition/anti-trust enforcement regime.

There may be special rules for public bodies. GDPR Article 83(7) allows Member States to lay down special rules for the public sector.

Given the potentially higher fines for infringements the data protection compliance drive for businesses will now be even more of an imperative.

Further reading:

See Fines Determination in GDPR Navigator.

Do some kind of privacy impact assessments have to be done?

Yes. Under GDPR these assessments are called Data Protection Impact Assessments (DPIAs). Where processing operations, in particular those using new technologies, *"are likely to result in a high risk for the rights and freedoms of individuals"*, an impact assessment of the envisaged processing operations on the protection of personal data must be carried out, prior to the processing, *"taking into account the nature, scope, context and purposes of the processing"*. GDPR also sets out other additional criteria that will require a DPIA.

A DPA must also be consulted prior to the processing of personal data where an assessment *"indicates that the processing would result in a high risk in the absence of measures taken by a data controller to mitigate the risk"*. DPIAs are likely to become more common and should prove to be a very useful tool for businesses in addressing privacy risks.

Further reading:

See our Privacy Impact Assessments: best practice and top tips video briefing.

Has anything changed with data transfers to third countries?

The core principles concerning the transfer of data from EU Member States to third countries (including the US) remain in place, including the requirement that those data transfers can only occur where an adequate level

of protection is assured by these third countries.

There remains a list of "whitelisted" countries which are considered as having an adequate level of protection for individuals' rights and to which personal data can be transferred in a relatively unrestricted way. What GDPR mainly introduces is an extension and more detailed treatment of the existing EU to third country data transfer principles.

The EU-US Privacy Shield programme has replaced the invalidated Safe Harbor as an approved mechanism for trans-Atlantic data transfers.

Binding Corporate Rules (BCRs) are put on an official footing and treated in-depth. Here, BCRs means *"personal data protection policies which are adhered to by a data controller or data processor established on the territory of a Member State for transfers or a set of transfers of personal data to a data controller or data processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity".*

The so-called "Model Contract Clauses" (or Standard Contractual Clauses (SCCs)) that impose obligations on both the exporter and the importer of the data to ensure that the transfer arrangements protect the rights and freedoms of data subjects remain a popular option as these can typically be put in place more quickly and cheaply than some other options.

Some of these transfer mechanisms (in particular, Privacy Shield and model clauses) are the subject of current court challenges to their validity. Therefore, it is always prudent to monitor developments and consider back-up options.

Further reading:

See Binding Corporate Rules in GDPR Navigator.

Where can I find GDPR?

Whilst GDPR is more commonly referred to as "GDPR" (i.e. the *"General Data Protection Regulation"*) the full official name of the new rules is "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)". The text of GDPR can be found in the EU Official Journal (OJ L 119 of 4.5.2016, p.1) at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG.

Cordery write regularly about data protection issues – please do check the Cordery News section of our website at http://www.corderycompliance.com/category/data-protection-privacy/ where we post our updates.

Please also note that these FAQS are highlights and by no means exhaustive of GDPR or of issues raised to them. GDPR is a complex area of law and you'll want to take specific legal advice on your own circumstances from a lawyer competent in this field.

What should we do now?

GDPR introduced a high level of compliance obligations, with significant financial, resource (including IT) and administrative costs. Every organisation's GDPR plan will be different but you might want to ensure that these ten elements are addressed:

1. maintain a DPIA process – map your data and determine areas of risk, and keep this under review;
2. thoroughly review your vendors' GDPR compliance capabilities and contracts – you will need your vendors' help in ensuring you can meet your GDPR obligations, especially in reporting security breaches very quickly. Make sure that you have the contractual rights to insist on this and make sure that you can hold your vendors to account;
3. ensure you have a GDPR-compliant data governance framework, including new detailed documentation and records that are ready for regulatory inspection –

of protection is assured by these third countries.

There remains a list of "whitelisted" countries which are considered as having an adequate level of protection for individuals' rights and to which personal data can be transferred in a relatively unrestricted way. What GDPR mainly introduces is an extension and more detailed treatment of the existing EU to third country data transfer principles.

The EU-US Privacy Shield programme has replaced the invalidated Safe Harbor as an approved mechanism for trans-Atlantic data transfers.

Binding Corporate Rules (BCRs) are put on an official footing and treated in-depth. Here, BCRs means *"personal data protection policies which are adhered to by a data controller or data processor established on the territory of a Member State for transfers or a set of transfers of personal data to a data controller or data processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity".*

The so-called "Model Contract Clauses" (or Standard Contractual Clauses (SCCs)) that impose obligations on both the exporter and the importer of the data to ensure that the transfer arrangements protect the rights and freedoms of data subjects remain a popular option as these can typically be put in place more quickly and cheaply than some other options.

Some of these transfer mechanisms (in particular, Privacy Shield and model clauses) are the subject of current court challenges to their validity. Therefore, it is always prudent to monitor developments and consider back-up options.

Further reading:

See Binding Corporate Rules in GDPR Navigator.

Where can I find GDPR?

Whilst GDPR is more commonly referred to as "GDPR" (i.e. the *"General Data Protection Regulation"*) the full official name of the new rules is "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)". The text of GDPR can be found in the EU Official Journal (OJ L 119 of 4.5.2016, p.1) at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG.

Cordery write regularly about data protection issues – please do check the Cordery News section of our website at http://www.corderycompliance.com/category/data-protection-privacy/ where we post our updates.

Please also note that these FAQS are highlights and by no means exhaustive of GDPR or of issues raised to them. GDPR is a complex area of law and you'll want to take specific legal advice on your own circumstances from a lawyer competent in this field.

What should we do now?

GDPR introduced a high level of compliance obligations, with significant financial, resource (including IT) and administrative costs. Every organisation's GDPR plan will be different but you might want to ensure that these ten elements are addressed:

1. maintain a DPIA process – map your data and determine areas of risk, and keep this under review;
2. thoroughly review your vendors' GDPR compliance capabilities and contracts – you will need your vendors' help in ensuring you can meet your GDPR obligations, especially in reporting security breaches very quickly. Make sure that you have the contractual rights to insist on this and make sure that you can hold your vendors to account;
3. ensure you have a GDPR-compliant data governance framework, including new detailed documentation and records that are ready for regulatory inspection –

factor this into overhead costs and ensure you have the resource to maintain this and monitor compliance;

4. review all key practical aspects such as data retention and destruction through all means of collecting data used by the business – the less data you hold, the less issues you are likely to have with GDPR (including with data subject rights);

5. ensure that aspects such as explicit consent, the right to be forgotten, and, the rights in relation to automated decision-making and profiling are all included in policies and procedures;

6. maintain an effective data breach notification procedure, including detection and response capabilities – also consider purchasing special insurance;

7. if applicable, appoint a DPO;

8. create compliance statements for annual business reports;

9. train staff on all of the above and provide regular refresher training; and

10. undertake regular compliance reviews or audits to identify and rectify issues.

Details of Cordery's data protection and privacy practice are at http://www.corderycompliance.com/data-protection-privacy/ and details of our training solutions are at http://www.corderycompliance.com/solutions/training/.

Appendix

Personal Data Processing Principles (as formulated under the new rules)

In summary, personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject
- Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date – every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; and,
- Processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

and:

- A data controller shall be responsible for and be able to demonstrate compliance with these six principles.

Cordery
Legal.Compliance