EU General Data Protection Regulation FAQs

This note is part of the Cordery GDPR Navigator.

Technical terms are used in this document which are explained in the glossary.

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

The EU has now changed its data protection rules. They were published in April 2016 and will fully apply from 25 May 2018.

These new rules are called the General Data Protection Regulation (or GDPR).

These changes go well beyond an upgrade. For all businesses there is now plenty to be done. Many deals being done now are likely to be governed by the new regime. Good planning from now will pay off to meet the eventual major compliance impact. These FAQs aim to help with that process.

What is EU data protection?

In the EU personal data can only be gathered under strict conditions and for legitimate purposes only – those who collect and manage personal information must protect it from misuse and must respect certain rights.

Data protection has up to now mainly been regulated in the EU under a 1995 Directive that controls the processing of personal data, which EU Member States had to implement into their own national legislation. Some countries had their own data protection laws prior to the 1995 Directive and there are differences in the way that the Directive has been implemented across Europe. These data protection laws have been of very wide effect with major compliance requirements placed on businesses inside and outside the EU – it should be stressed that data transfers outside the EU have in particular been under the spotlight in the Schrems Safe Harbor ruling of the European Court, which we reported on at http://www.corderycompliance.com/european-court-rules-safe-harbor-invalid-in-schrems-case/.

Why the change?

The data world of 1995 was significantly different to today and so a significant overhaul was needed in order to catch up with the huge advances of the digital age. 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. Those promoting the GDPR also hope that being more privacy-friendly will enhance business competitiveness.

Are these completely new rules?

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

What new rules will there be?

The new rules are in the form of a Regulation, which has been chosen as the legal format (as opposed to a Directive) so that the EU data protection rules should be the same in all 28 EU Member States – no further legislation will be adopted by EU Member States to make this Regulation the law in their national systems.

This said, the Regulation allows some latitude for the 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, or, in unaddressed areas, including processing data concerning deceased persons. In addition, Member States like the UK will be faced with the legislative issue of what to do with certain existing aspects of their national data protection rules that are additional to the rules set out in the 1995 Directive.

So, it is likely that in each EU Member State there will be: the "core" data protection rules as set out in the Regulation; and, some additional "local" rules. Whilst the main focus for businesses will be the "core" rules, which will be the same throughout the EU and should make the compliance task more straightforward, in order to ensure full compliance, businesses should also check for any local variances.

My business is not in the EU so will these rules still affect me?

Yes. The new rules will apply not only to businesses which are actually located in an EU Member State, but, also, to businesses located completely outside the EU. This will be the case where:

- Either, a business processes the personal data of EU residents and offers them goods and services, irrespective of whether payment is required; or,
- Where the processing by a business relates to the monitoring of the behaviour of EU residents in so far as their behaviour takes place within the EU.

The new rules state 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 the new rules. But, the new rules also state that factors such as 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 the mentioning of customers or users who are in the EU, may be factors to indicate that a business envisages offering goods or services to EU residents, and thereby bring the business within the scope of the new rules.

For a business located outside the EU, where its data-processing is neither occasional nor large-scale for certain data, it will have to designate (in writing) a representative in the EU where the data subject EU residents are and whose personal data is processed either in relation to the offering of goods and services or whose behaviour is monitored. The representative should be explicitly designated by a data controller or processor to act on their behalf concerning their obligations under the new rules, although the designation of a representative does not affect the responsibility or liability of the controller or processor under the new rules. The representative should perform their tasks according to the mandate received from the controller or processor, including co-operating with the national regulators, and the representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

This extra-territorial dimension is a very significant change, but, it may nevertheless be very challenging for national regulators in the EU to actually enforce.

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

Under the new rules national independent regulators will remain in place, i.e. there will not be a single centralised EU regulator. A key aspect of the changes is that a business, referred to as an "establishment" under the new rules, should only have to deal with one data protection regulator (i.e. a one-stop-shop), which is called a "supervisory authority" under the new rules.

To enable a business to deal with just one regulator, under the new rules, the "supervisory authority" of either the *main* "establishment", or, (if this is the case) of the *single* "establishment" of a data controller or processor, will act as "*lead* supervisory authority" in situations where data-processing carried out by that controller or processor is *cross-border*, i.e. it cuts across EU Member States. A particular EU co-operation procedure between "supervisory authorities" will apply in such instances, i.e. the

"*lead* supervisory authority" will work closely with the other "supervisory authorities" on the matter in question.

As an exception to the situation immediately above, in the case of an infringement of the new rules or where someone lodges a complaint whose subject-matter relates *only* to an "establishment" in *its* EU Member State or substantially affects data subjects *only* in *its* EU Member State, then in these cases *each* "supervisory authority" will have the competence to handle the infringement or complaint in question. Here too particular procedures will apply, including within the context of the above-mentioned EU co-operation procedure, between the "supervisory authority" and the "*lead* supervisory authority" as regards the handling of the matter in question.

The to-be-created (independent) "European Data Protection Board" (which will replace the current "Article 29 Working Party", an important grouping of the EU data protection regulators) will also have as one of its functions to act as a dispute resolution mechanism concerning disputes between regulators, notably between the "*lead* supervisory authority" and other "supervisory authorities."

It should also be noted that the effect of the European Court ruling in the Weltimmo case, (which we have written about at http://www.corderycompliance.com/european-court-weltimmo-ruling-on-the-jurisdiction-of-data-protection-regulators/), is that a business operating through the internet cannot base itself in one jurisdiction and ignore the regulators in other EU Member States if it is targeting its online business to those other countries.

So, businesses will have to deal with one regulator but this regulator may well be interfacing with other regulators. This one-stop-shop approach is a welcome step forward in terms of simplifying compliance and ensuring consistent application of the new rules by regulators, but, because of its nature the co-operation procedure may also lead to administrative and bureaucratic delays for businesses.

Will I have to register with a regulator?

No. There will no longer be a requirement for a data controller to register with a data protection regulator, and consequently the payment of a fee to register will also disappear. But, just as one regulatory obligation disappears another one takes its place! Where the new data protection impact assessment process applies (see later below) a data protection regulator 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.

The disappearance of general registration will also pose a challenge for some Member State regulators who will lose an income stream from fees for registrations. This may impact their budgets and affect their administrative and enforcement capabilities, unless they can increase their revenue by levying substantial fines.

Will data controllers and processors have more to do?

Yes, data controllers and processors will have considerably more responsibilities and obligations under the new rules. Processors will now have direct obligations, and, exposure to fines under the new rules.

A 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 the new rules, including the implementation of data protection policies.

Controllers and processors will have to maintain records of processing activities, according to detailed criteria set out under the new rules, which must be made available to "supervisory authorities" upon request.

The new rules also stipulate that processing by a processor on behalf of a controller must be set out in a contract or "other legal act", according to certain criteria laid down under the new rules.

An important practical upshot 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.

Will I have to make privacy an integral compliance element in my business?

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

The practical upshot is that data controllers will have to implement appropriate technical and organisational measures for data processing, such as "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.

Controllers will 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 encompass 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 natural persons.

The practical application of these measures will require time and effort on the part of a business to implement.

Will consent be required for data processing?

Yes. The requirements for consent have also been recalibrated. The new 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 will not be able to rely on silence or opt-outs and instead an active process such as box-ticking will have to be put in place – according to the new rules "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.

Under the new rules, as regards 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; EU Member States may provide for a lower age for these purposes, but not 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.

Consent is a feature that businesses will therefore have to pay special compliance attention to.

Are there any new rights?

Yes. A series of new rights have been introduced.

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 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", subject to certain conditions set out under the new rules.

There is what is more commonly being referred to as the "Right not to be Profiled". 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.

There is also now a legislative "Right To Be Forgotten", 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; note that a judicial "Right To Be Forgotten" was also set out 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.

These new rights will be challenging to implement, although it should also be emphasized that all these new rights are qualified, i.e. they are not absolute and have their limits.

Further, it should also be noted that under the new rules, so-called "Subject Access Requests" (SARs), a process whereby someone can exercise their right to gain access to data held on them, must be answered within one month of receipt of the request, but which may be extended for a maximum of two further months when necessary taking into account the complexity of the request and the number of requests. It must also be highlighted that under the new rules the ability for a business has to ask for a fee for an SAR has been abolished. There has been a significant rise in the number of SARs being made in recent years – when SARs become free an even greater rise in requests can be expected. Given the prevalence of email and cloud applications in particular, SARs are also now more costly and complex to deal with. An illustration of that complexity would be 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 future data protection strategy will therefore be putting proper processes in place to deal with SARs.

Will I 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 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,
- The core activities of the data controller or the processor consist of processing on a large scale of special categories of personal data, namely those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and, the processing of genetic and biometric data in order to uniquely identify a person, or data concerning health or sex life and sexual orientation (which can only be processed under certain strict conditions such as where consent has been given), or, data relating to criminal convictions and offences.

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 will report directly to the highest level of management.

Businesses will therefore have to determine whether a DPO must be appointed or not, but, given the significance of privacy compliance today, even if technically-speaking a DPO is not required to be appointed, a business of a particular size that regularly processes data may wish to consider appointing one in any event.

When will I have to report data breaches?

Ensuring that data is secure is one of the backbones of the new law. Significant changes concerning the mandatory reporting of data breaches have been introduced requiring reporting to the regulator and communication to those affected.

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.

Breaches will have to be reported, under conditions set out in the new rules including what action has been done to mitigate them, to the relevant data protection regulator 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.

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", which must be done 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 have 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 to be implemented across the EU in line with the EU Cyber Security Directive, which is expected to be finalized mid 2016 (for more details see our alert at http://www.corderycompliance.com/eu-cyber-security-rules-agreed/).

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

What about liability and compensation?

As a general principle, any person who has suffered "material or non-material damage" due to an infringement of the new rules has a right to compensation from the data controller or processor concerned for the damage suffered – defences to liability are also set out under the new rules.

Generally the issue of liability for data protection infringements is a growing topic. Important legal issues in this area have arisen in the UK case of Vidal-Hall that are expected to be finally resolved this year by the Supreme Court, which we have written about at http://www.corderycompliance.com/uk-supreme-court-allows-google-to-appeal-in-vidal-hall-data-protection-liability-case/. In addition, Austrian proceedings against Facebook have been brought by Max Schrems, which we reported on as continuing at http://www.corderycompliance.com/schrems-class-action-to-continue/.

Because of the extra risk that a data infringement may now entail under the new rules, 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 the new rules regulators may "carry out investigations in the form of data protection audits", and, they may "obtain access to any premises of the controller and the processor, including to any data processing equipment and means" in line with relevant procedural law (obtaining a warrant etc.). This seems to apply equally to the private and public sectors. This may prove to be a significant tool in the data protection regulators' armoury. Businesses therefore need to put in place procedures and train staff to deal with this.

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

Under the new rules, data protection regulators will have the power to impose high fines for infringing the new rules. Different bands of fines will be applied in relation to three different sets of categories of infringements – the highest level of fine is either a maximum of Euro 20 million or 4% of the global annual turnover of a business, whichever is the greater, which will apply to the second and third categories of infringements. As regards consideration of aggravating and mitigating factors the approach that will be taken is very much on the lines of EU competition/anti-trust enforcement.

There may be special rules for public bodies. 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.

Will some kind of privacy impact assessments have to be made?

Yes. Under the new rules 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." The new rules also set out other additional criteria that will necessitate an impact assessment.

A data protection regulator 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 common and should prove to be a very useful tool for businesses in addressing privacy risks.

Has anything changed as regards 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.

What the new rules mainly introduce is an extension and more detailed treatment of the existing EU to third country data transfer principles. Of particular note here is that so-called "Binding Corporate Rules" are put on an official footing and treated in-depth. Here, Binding Corporate Rules means "personal data protection policies which are adhered to by a data controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity". As we have highlighted at http://www.corderycompliance.com/european-court-rules-safe-harbor-invalid-in-schrems-case/ following the 2015 Schrems Safe Harbor ruling of the European Court, "Binding Corporate Rules" may well be the future as regards EU to third country data transfers, with other arrangements put in place in the meantime such as so-called "Model Contract Clauses" 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. As at the date of these FAQs the regime that may replace Safe Harbor, EU-US Privacy Shield, is still not a viable option.

Where can I find the new rules?

The new rules are now more commonly being referred to as the "GDPR" (i.e. the "General Data Protection Regulation") although 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)" which 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. We write regularly about data protection issues – please do check 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 the new rules nor of issues raised by them.

What should I do now?

The new rules will bring a high level of compliance obligations, with significant financial, resource (including IT) and administrative costs. Use your planning time well to adapt to them – the following are ten top compliance issues to start addressing:

1. Put in place a privacy impact assessment process – map your data and determine areas of risk;
2. Thoroughly review vendor contracts – you will need your vendors' help 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. Prepare to update everything and prepare new detailed documentation and records ready for production for regulatory inspection – factor this into overhead costs;
4. Review all key practical aspects such as data retention and destruction through all means of collecting data used by the business;
5. Ensure that new aspects such as explicit consent, the right to be forgotten, and, the right to not be subject to profiling are all included in policies and procedures;
6. Put in place a data breach notification procedure, including detection and response capabilities – also consider purchasing special insurance;
7. If applicable, appoint a data protection officer;
8. Create compliance statements for annual business reports;
9. Train staff on all of the above; and,
10. Set up and undertake regular compliance audits in order 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 sum, 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.