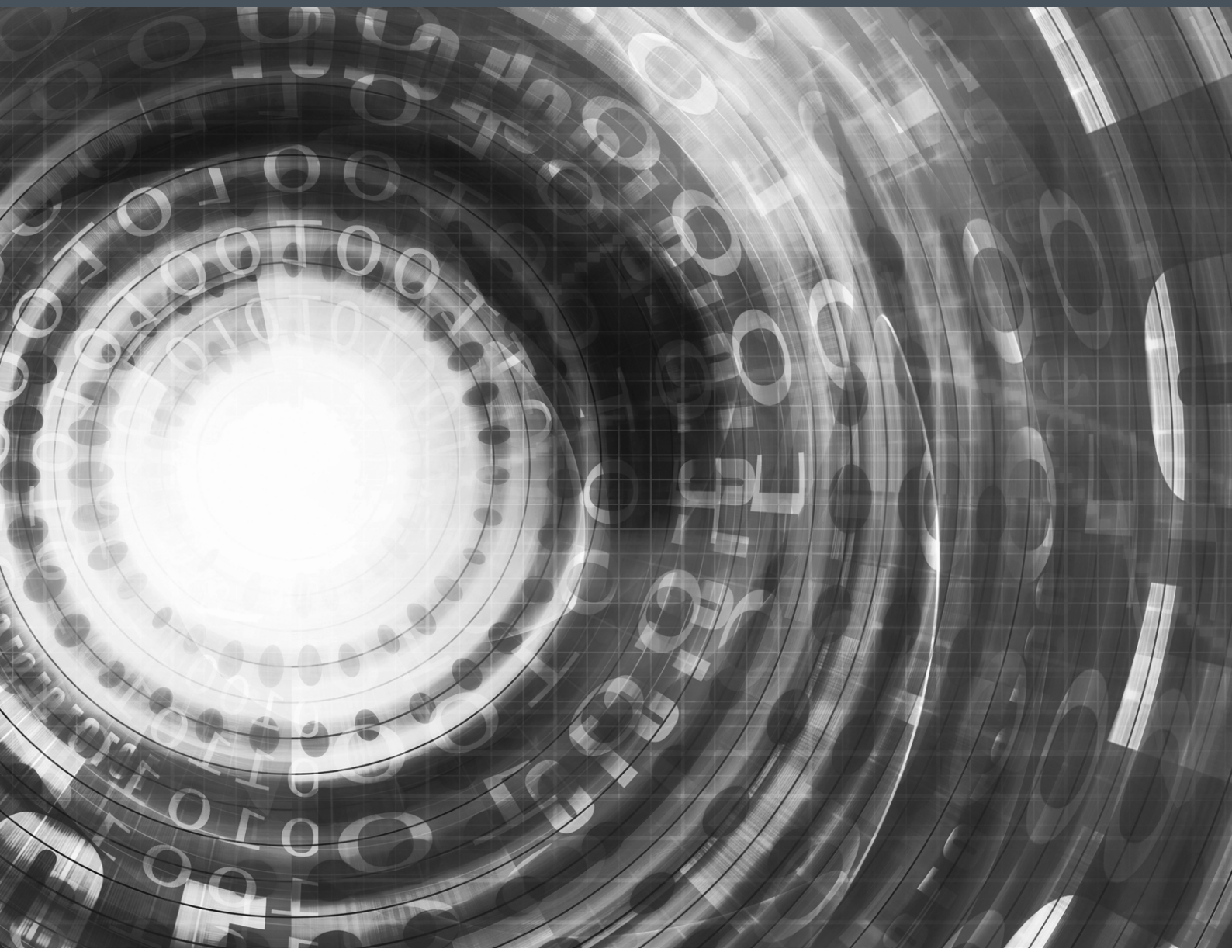

ALL CHANGE – ARE YOU COMPLIANT WITH THE EU GENERAL DATA PROTECTION REGULATION?

SPECIAL UPDATE

Organisations (including many outside the EEA) have now had more than three months to get used to the EU General Data Protection Regulation (GDPR), which overhauled a data protection regime dating from 1995.

The GDPR became effective across the European Economic Area (EEA), including in the UK, from 25 May 2018. It also applies to a large number of organisations established outside of the EEA. With risks of large potential fines (up to 4% of global turnover or €20 million, whichever is greater), claims from individuals and reputational damage, organisations need to make the necessary changes now to their business practices, if they have not already, in order to be "GDPR compliant".

"The GDPR is implemented in the UK by a new Data Protection Act 2018 which is intended to go beyond the GDPR in setting 'the gold standard on data protection'".

Under the GDPR the obligations on data controllers have substantially increased and processors also have data protection obligations. For example, in accordance with a new focus on accountability, controllers and processors are required to keep records of their processing. Contracts with processors need to be updated to include new mandatory provisions. Privacy notices need to be updated. 'Consent' is more difficult to obtain and may need to be refreshed. Principles of 'privacy by design' mean that organisations must look at their processing and assess whether it is really necessary. Under the new definition of personal data, online identifiers such as cookies and IP addresses can make an individual 'identifiable'. The definition of 'sensitive' ('special category', in GDPR terms) personal data also contains new elements such as genetic data. We discuss below some of the key elements that require action if they have not already been addressed.

Application outside of the EEA

International organisations cannot afford to ignore the GDPR just because it originates in the EU. The GDPR applies to a non-EEA organisation if it has a presence in the EEA, or it is established outside the EEA and monitors the behaviour of individuals within the EEA (for example via cookies) or it offers products or services to individuals within the EEA. It also applies where EEA Member State law applies in accordance with international law. Coupled with the fact that the GDPR also imposes obligations on processors, this EU Regulation significantly widens EU regulators' jurisdiction. Controllers or processors established outside of the EEA but to whom the GDPR applies must appoint a representative within the EEA.

GDPR in the UK post Brexit?

The GDPR will continue to be applicable in the UK post Brexit, just as other EU Regulations will, as 'retained' law.

The GDPR is implemented in the UK by a new Data Protection Act 2018, which is intended to go beyond the GDPR in setting *"the gold standard on data protection"*. The UK Data Protection Act sets the UK's exemptions, its enforcement mechanisms, and any criminal penalities. For example, the UK Act introduces criminal offences for intentionally or recklessly re-identifying individuals from anonymised or pseudonymised data, and for altering records with the intent to prevent disclosure following a subject access request. Although the GDPR is intended to be a 'one stop shop', all EEA Member States will have a data protection law to set out their enforcement mechanisms and to use their discretion on certain elements of the GDPR where this is permitted. Germany, for example, approved a new Data Protection Act in May 2017.

So what should you do?

We discuss below nine key issues to consider when complying with the GDPR, and some immediate steps which businesses should take in order to deal with them. You can also find a brief overview of some of the main provisions of the GDPR in our client alert of April 2016[1].

1. Controller or processor – what are your obligations?

Whilst the definitions of controllers and processors have not changed, processors are also liable for some, but not all, elements of the GDPR. Contracts must be in place with processors, which must include a number of mandatory provisions, set out in Article 28 of the GDPR.

Since the penalties for non-compliance are much higher, businesses should take stock of their legal status and obligations, and revisit their contracts with service providers.

1. http://www.hfw.com/Data-protection-has-new-teeth-April-2016

Under the GDPR it is controllers who make the decisions on how and why data are processed whereas processors act only on the instructions of the controller. Businesses may act as a controller or as a processor in respect of different data sets, as may their service providers.

If a business only collects and processes personal data on its own behalf then the analysis is simple: it is a controller. However, classification becomes trickier when it processes personal data on behalf of customers. It is possible in such circumstances that it could be either a 'joint controller' or a processor for the data it processes on behalf of its instructing party. It could also be a combination of the two (ie. a joint controller for some data and a processor for other data). Separately, it will be a controller for the data about its own customer – for example the names and email addresses of the individuals working for its instructing party. 'Joint controllers' must make arrangements between them to ensure individuals' rights are protected.

Action required

- Make sure that at the outset of any business relationship you have fully considered whether you will be acting as a controller or a processor, and document your assessment accordingly.
- Make sure that your status is reflected in any contractual documentation.
- Given that controllers have more responsibilities, you may prefer to remain a processor if you can, but remember that whether you are a processor is a question of fact and law rather than a label under a contract.

2. Grounds for processing – beware 'consent'

The processing of personal data is prohibited under the GDPR unless a controller has one or more of the legal grounds for processing that data. For standard personal data which is not sensitive, the grounds are:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
- 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.
- Processing is necessary for compliance with a legal obligation to which the controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person (ie. to save a life).
- 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 controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the 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.

The grounds for processing sensitive ('special category') personal data (for example data which could reveal information about an individual's ethnic or racial origin, religious beliefs, health or sex life/sexual orientation) are more limited. There are also special rules for information about an individual's criminal records, which is generally not permitted unless there is a local law that justifies it.

For sensitive personal data, with some exceptions, the individual's consent is necessary unless the individual's life is at risk (or other peoples' lives are at risk) and the individual is not able to give consent. Other grounds include processing which is necessary for reasons of substantial public interest on the basis of EU or Member State law (in the UK, see the UK Data Protection Act 2018), or processing which is necessary for the establishment, exercise or defence of legal claims, but these grounds can be difficult to rely on and must be carefully justified and documented. There are no applicable "*legitimate interest*[2]" or "*necessary for the performance of a contract*" grounds for sensitive personal data.

The GDPR tightens the 'consent' ground for processing, which applies to both types of personal data but especially to sensitive personal data. The GDPR clarifies that if relying on this ground, controllers must be able to demonstrate that an individual has consented to the processing of his or her data. Consent provisions cannot be buried in the middle of a long piece of text and must be a clear affirmative indication of the individual's wishes. In addition the recitals clarify that consent must be able to be withdrawn at any time.

Action required

- Where you currently rely on consent for processing any type of data you should check whether there are other applicable grounds that you can rely on instead.
- Check that you have records of your customers' and employees' consent, that you do not collect this kind of data unless absolutely necessary, and that you do not keep it longer than necessary.
- Check that each individual (natural person, sole trader or unlimited liability partnership) on your marketing databases has either explicitly consented to receive electronic marketing, or if they are existing customers that they were given the opportunity to opt out from such marketing when their contact details were first collected and that their wishes have been respected. Note that there will be specific provisions on electronic marketing in the forthcoming ePrivacy Regulation. As currently drafted, the proposed ePrivacy Regulation keeps the 'soft opt in' currently available under the ePrivacy Directive. However, this is subject to change until the text is finalised.

2. There is a very limited '*legitimate interest*' ground for charities however.

"Where businesses process personal data which they have not received from the individuals directly they must ensure that the individuals know that they are doing so."

- For business contacts (ie. individuals with business email addresses), properly assessed and documented legitimate interest may be a more appropriate ground than consent for the purposes of direct marketing, but beware ePrivacy rules if you are using electronic communications, and ensure that each communication includes a mechanism to 'opt out' of future unsolicited marketing. This is to ensure that these data subjects can easily exercise their right to object to their personal data being processed for marketing purposes.

3. Data audit and record keeping requirements

The GDPR has a particular focus on accountability and transparency. It is no longer sufficient to comply with the law, businesses must be able to demonstrate that they have done so with appropriate records and evidence.

Controllers generally no longer have to 'register' with local data protection authorities[3] but, instead, are required to keep and maintain records of their processing including for example: the purposes of processing; the data subjects and categories of personal data involved; details of personal data transferred outside of the EEA; the envisaged time limits for deletion of different categories of data; and a general description of the technical and organisational security measures it uses to keep personal data safe. These records must be available for inspection by a relevant EU data protection authority on request.

Processors also need to keep (more limited) records of their processing, including for example details of what kinds of data they process for whom, what data are transferred outside of the EEA, and a general description of the technical and organisational security measures it uses to keep personal data safe.

Where organisations have fewer than 250 employees the record-keeping requirements may not apply to some processing operations.

Action required

- Audit your personal data if you have not done so. What personal data do you process? Why did you collect them? Why and how are you using them? Where are they kept? Do you have extensive personal data in archive? Do you still need them? Do you now use them for new purposes?

If personal data are out of date or no longer needed, delete or anonymise them.

4. Fair processing notices – privacy policies

Data subjects must be kept informed about the processing of their personal data. The GDPR increases the amount of information which must be included in these notices. For example, if data controllers are relying on the ground of 'legitimate interests' in order to process personal data then the individuals must be informed at the outset of what those legitimate interests are.

In addition, the privacy notice must point out to the individuals their GDPR rights, including the right to withdraw consent at any time and the right to lodge a complaint with a supervisory authority.

Where businesses process personal data which they have not received from the individuals directly they must ensure that the individuals know that they are doing so. There is a list of information which must be provided to individuals in these circumstances (for example the categories of personal data that are being processed, the source the personal data originate from and whether they came from publicly accessible sources).

Action required

- Make sure that your privacy notices are up to date with the GDPR requirements.
- Consider 'just in time notices' (such as a box of text which appears when a mouse hovers over a particular box in a collection form) when collecting personal data such as email addresses to say how that information will be used.
- If you collect information on individuals from third parties then make sure that the individuals are aware of this. Where this is technically difficult, explore contractual options with the entities which provided the data to you to ensure that individuals are kept up to date and know how to enforce their rights.

5. Additional and strengthened rights for individuals

The GDPR strengthens and increases individuals' rights. Some examples are as follows:

- Subject access requests. The information which must be provided to an individual who makes a genuine subject access request has been increased (for example it must now include a notification of the right to lodge a complaint with the supervisory

3. Although there may still be an obligation to pay fees to the local supervisory authority - in the UK the ICO requires many controllers to pay fees.

authority, and information about transfers of the data outside of the EEA). Organisations have a shorter period of time to respond: the response must be 'without delay' or at least within one month of receipt of the request (the old response period was 40 days).

- Right to request deletion. The controversial 'right to be forgotten' has been strengthened, specifying the circumstances where the controller must on request erase personal data without 'undue delay' (for example where processing is based on the individual's consent but the individual has decided to withdraw that consent – another reason to avoid using consent as legal grounds for processing).
- Data portability. There is a new right to 'data portability' for data which was provided directly by the individual and where the processing is based on consent or on the carrying out of a contract and the processing is carried out by automated means (ie. on computers or other devices). The data should be provided to the individual in a structured, commonly used and machine-readable format and the individual will have the right to transmit the data to another controller.
- Right to object to processing. Individuals have a right under the GDPR to object to their data being processed where the processing is carried out using the legal grounds: (a) that the processing is necessary for the performance of a task carried out in the public interest; or (b) where the processing is necessary for the purposes of the legitimate interests of the controller or a third party. A controller can continue to process the data if it can demonstrate *"compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject"* or if the processing is necessary for the establishment, exercise or defence of legal claims.
- Right to object to direct marketing. Individuals have an absolute right to object to their personal data being processed (including storage) for direct marketing purposes.
- Right to request restriction. Individuals will also have the right to request that their data be 'restricted'. This effectively means that a data controller will not be able to use the data in question until it has decided whether or not the individual's claim is genuine or can be refused.

Action required

- Put processes in place to deal with requests from individuals seeking to enforce their rights within the shorter period permitted for response, including a designated team to deal with such requests. On receipt of a request from an individual, the quicker that you can make a decision the sooner you can resume business and minimise the waste of company time and resources.

6. Contracts with processors

As mentioned above, the GDPR requires data controllers to add certain clauses to their contracts with all data processors. Additional clauses under the GDPR include, for example, an obligation on the data processors to act only on the documented instructions of the data controller, to impose confidentiality obligations on the staff who will be processing the data and to delete or return all of the personal data at the end of the provision of services related to the processing.

Action required

- Consider which of your service providers are acting as data processors and which are acting as controllers.
- Check whether you are a 'joint data controllers'.
- Make sure that your contracts contain the necessary GDPR elements.

7. Reporting of personal data breaches

Controllers' duty to notify the relevant data protection authorities:

- Under the GDPR a controller must notify a personal data breach to the relevant supervisory authority within 72 hours after becoming aware of a personal data security breach.
- The exception to this is where the data breach is *"unlikely to result in a risk to the rights and freedoms of natural persons"*.
- Where there is such a risk, a delay beyond 72 hours must be accompanied by reasons for the delay.

Controllers' duty to notify the individuals concerned:

- When the personal data breach is *"likely to result in a high risk to the rights and freedoms of natural persons"* the data controller must also notify the data subject *"without undue delay"*. This could be a smaller notification window than 72 hours.

Processors' duty to notify the controller:

- Processors have a direct obligation under the GDPR to notify the data controller *"without undue delay"* on becoming aware of a personal data breach.

This is a key change. The previous EU Directive did not generally require controllers to notify data protection authorities about security breaches (although telecommunications service providers were required to do so under the ePrivacy Directive and some Member State laws may have required such notification). Under the GDPR, notification is mandatory and as explained above the timelines are short for compliance.

In addition to the notification requirements, controllers need to keep a register of any personal data breaches, including details of what happened and what was done to resolve the issue. This will be subject to inspection by the relevant supervisory authority.

Action required

- Create and maintain a register of data breaches.
- Update your cyber security breach procedures to take into account the short timelines for notification under the GDPR.
- If you do not already have such a procedure in place, consider creating one. In the event of a security breach there will be very little time in which to determine the extent of the damage, the individuals affected, the security arrangements which will need to be either changed or strengthened, and whether or not the breach requires notification to the national data protection authority and/or individuals concerned. A breach will be less painful if you take steps now to establish parameters for making such decisions, and identify the people who will be responsible for making them.
- Consider whether you have appropriate cyber security insurance in place and line up public relations advisors who can help you to reduce the damage to your reputation in the event of a personal data breach.

8. 'Privacy by design' and Data Privacy Impact Assessments

An important new concept is that of 'privacy by design and by default'. When introducing new products, services, or processes, controllers need to show that the impact of such products, services or processes has been considered, and that steps have been taken to minimise any negative impact. Data should be pseudonymised where possible and should not be collected unless it is really needed.

Action required

- Do not collect personal data unless you can justify your purposes. If any envisaged processing operations are likely to result in a 'high risk' to the individuals, conduct privacy impact assessments. These should, amongst other things, determine how you will keep personal data safe.
- Make sure that your internal data protection policies are up to date and that your data processing is transparent.

9. Appointment of Data Protection Officers and representatives

Although there is no longer generally a need to register as a controller in an EU Member State, controllers and processors must designate a 'data protection officer' in certain circumstances, including where:

- The 'core activities' of the controller or the processor consist of "processing operations which… require regular and systematic monitoring of data subjects on a large scale"; or
- The 'core activities' of the controller or the processor consist of *"processing on a large scale"* of *"special categories of data"* (ie. 'sensitive personal data') and *"personal data relating to criminal convictions and offences"*.

A controller or processor can also choose to appoint a data protection officer voluntarily, or a Member State can require it under local law. Given the increasing importance of data protection, it can be useful to dedicate resources to ensuring compliance with applicable data protection laws. However, be aware that there are mandatory minimum requirements under the GDPR for data protection officers, for example the data protection officer should have expertise on both local data protection law and on the GDPR. Organisations established outside of the EA must appoint a representative within the EEA if the GDPR applies to them, with some exceptions.

"If you have not already completed your GDPR preparations you should work quickly to put at least the most important provisions in place."

Action required

- Assess whether you should appoint a data protection officer.
- Consider whether you have appropriate staff for this, or whether you need to hire a new officer, or outsource the role.
- If your organisation is established outside of the EEA, appoint a representative within the EEA unless one of the exceptions applies.

Why should businesses comply with the GDPR?

Getting this right means that businesses are more likely to attract and retain their clients and customers. Marketing will be more effective and efficient and businesses will be better able to gain and maintain the trust of clients and employees alike.

On the other hand, the penalties for getting this wrong are potentially very high. National supervisory authorities have the power to impose fines of up to 20 million Euros, or 4% of the total worldwide turnover of a business in the preceding financial year, whichever is higher. Member States must also lay down rules on other penalties applicable to infringements of the Regulation, and must take *"all measures necessary to ensure that they are implemented… such penalties shall be effective, proportionate and dissuasive"*.

If you have not already started your GDPR preparations you hould work quickly to put t least the most important provisions in place. The key point is to assess the areas where your business is particularly at risk and prioritise your preparations accordingly. Clean your marketing database and make sure that requests to unsubscribe are respected. Check that personal data is being processed lawfully, in particular sensitive personal data. Make sure that transfers outside of the EEA are lawful, and check that your systems are secure. At the same time as doing all of this, conduct a thorough data audit so that you know what you have and what you do with them, and record your findings in a set of 'records of processing activities' that can be produced to the national supervisory authority on request. Above all, document the process – the GDPR requires businesses to demonstrate that they are complying.

Act now, unless you want to risk being an enforcement case that makes headlines.

For further information please contact:

ANTHONY WOOLICH
Partner, London
T +44 (0)20 7264 8033
E anthony.woolich@hfw.com

FELICITY BURLING
Associate, London
T +44 (0)20 7264 8057
E felicity.burling@hfw.com

JEREMY KELLY
Associate, London
T +44 (0)20 7264 8798
E jeremy.kelly@hfw.com

HFW has over 550 lawyers working in offices across Australia, Asia, the Middle East, Europe and the Americas. For further information about our EU, competition and regulatory trade capabilities, please visit hfw.com/EU-Competition-and-Regulatory

hfw.com

Americas | Europe | Middle East | Asia Pacific