
CLIFFORD
CHANCE
NEW EU GENERAL DATA PROTECTION REGULATION
THE BIGGEST CHANGE IN PRIVACY LAW IN A GENERATION

CONTENTS

THE BIGGEST CHANGE IN PRIVACY LAW IN A GENERATION

The EU General Data Protection Regulation (GDPR) was passed in 2016 and will become law on 25 May 2018. It represents the biggest change in EU data privacy law in a generation and is likely to form a model for new data privacy rules in other jurisdictions.

The GDPR preserves and builds on the principles of the current EU regime, which was designed for a pre-digital age. It seeks to achieve greater legal consistency across the EU and the wider European Economic Area (EEA), and at the same time introduces a raft of new aggressive and intrusive rules. In particular, there are very serious sanctions for breach, including fines which can go as high as 4% of the global turnover of a group of companies.

The new law places protection of the privacy rights of the individual at its centre and, in the process, runs contrary to many business models that assume that data can flow freely, and without restriction in its use.

Adjustment to the new regime will require radical changes in approach for most businesses. Make no mistake, if companies do not prepare, they will be exposed to an unprecedented regulatory risk. The value of one of the most important assets a business holds – data – could be severely diminished without careful planning.

In this short briefing note we identify the key changes being introduced by the GDPR and summarise the practical steps that need to be taken to effectively build the GDPR into your compliance culture.

Jonathan Kewley
Partner

Dessislava Savova
Partner

Richard Jones
Director of Data Privacy

UNPRECEDENTED SANCTIONS AND REMEDIES FOR BREACH

The GDPR substantially increases the risks associated with failure to comply with the EU data privacy regime by increasing the potential sanctions for breach. Even without all the significant changes being made to the substantial requirements of the regime, this – together with the ever increasing appetite for protection of privacy across Europe – would be sufficient to transform the European data privacy environment.

Potential sanctions fall into the following categories – sanctions in all of these categories could potentially be imposed under the current regime, but the GDPR will be much more aggressive in several key respects:

Administrative fines: These are not mandatory under the Directive. Under the GDPR, a scheme of fines based on the anti-trust model will be introduced:

- for serious breaches, up to the higher of EUR 20 million and 4% of group global turnover
- for less serious breaches, up to the higher of EUR 10 million and 2% of group global turnover

For large organisations, of course, these fines are potentially huge.

Civil sanctions: As under the current regime, individuals will be able to claim compensation through the civil courts for damage or distress suffered as a result of breaches. There are new provisions allowing data subjects to nominate not-for-profit organisations to bring claims on their behalf, opening the possibility of class actions for breach.

Regulatory action: Data protection authorities will have clear audit rights (only patchily available under the Directive) and, as under the Directive, will have various powers to compel compliance with the GDPR.

Criminal penalties: Member states will remain free to impose criminal penalties for breach.

THE FUNDAMENTALS OF EU DATA PROTECTION LAW

Why replace the existing regime?

The European Union already has a comprehensive and onerous data protection regime, introduced in the late 1990s and early 2000s by EU Directive 95/46/EC (the Directive) and its national implementing laws in each EU member state.

Technology was less advanced and ubiquitous when the Directive was drafted than it is today. In the late 1990s, the data privacy implications of the processing of personal data were not fully understood. Attitudes to data, privacy, technology and business objectives have moved on. There is also a perception that the Directive failed to create a harmonised data protection regime across the EU, and that businesses and others have not fully bought in to its principles – it is argued that the existing rules need to be backed up by "accountability" principles, requiring those responsible for the processing of personal data to build data privacy considerations into their business processes and the design of their IT systems.

The changes to be introduced by the GDPR are incremental, preserving substantially all of the fundamental principles of the current regime but tightening them and adding a series of new supporting principles. The sanctions for breach will also be substantially increased. The result is a very comprehensive and strict data protection regime, unparalleled in the scope and weight of the compliance burden that it places on businesses and other organisations reliant on the processing of personal data.

"Processing" of "personal data"

EU data protection law seeks to protect the privacy of "*data subjects*" (i.e. individuals) with regard to the "*processing*" of their "*personal data*". Neither the Directive nor the GDPR protects information relating to companies or other legal persons.

"Personal data" is extremely broadly defined. It covers all information relating to identifiable individuals which is held either in electronic (or other automatically-processable) form or in a structured manual filing system. It includes information about an individual's private life but also relatively trivial information such as an employee's work contact details. The approach taken – and this does not change under the GDPR – is not to focus on particularly sensitive data processing (e.g. for the purposes of employee behaviour monitoring or spam marketing) but to apply a series of general principles to a very wide range of processing.

Examples of "personal data"

Data held by an employer about its employees, including in their professional capacity

Data held by a business about its individual customers

Data held by a company about the employees of its corporate customers or suppliers (e.g. taken from their business cards)

Who must comply?

- The Directive and GDPR both impose obligations on so-called "*controllers*", who determine the purposes and means of processing of personal data
- Controllers are distinguished from "*processors*" – service providers who process data on behalf of their controller-customers
- The Directive does not directly regulate processors although it requires controllers to impose data security obligations on them by contract. This will change under the GDPR

THE FUNDAMENTALS OF EU DATA PROTECTION LAW

The unchanging principles

The key data protection principles underpinning the current regime and repeated in the GDPR include:

(a) ***legitimacy***: all processing of personal data must be justified by meeting one of the conditions set out in the law, which include:

  (i) the data subject's **consent**

  (ii) processing being necessary for compliance with an obligation arising under (EU or member state) **law**

  (iii) the so-called **"legitimate interests"** condition, which allows processing which is necessary so that the controller can pursue its legitimate (business or other) interests if those interests outweigh any related prejudice to the privacy of the data subjects – a balance needs to be struck between the interests of the controller and the data subject

(b) ***fairness and proportionality***: all processing must be fair, proportionate and compatible with the purposes for which the data were collected, and data must be deleted when they are no longer needed

(c) ***transparency***: data subjects must be told about the processing of their information and given other information as necessary so that the processing is fair

(d) ***accuracy***: reasonable steps must be taken to ensure that personal data are accurate and, where relevant, up to date

(e) ***security***: personal data must be protected by appropriate security measures

There are limited exceptions to all of these principles.

The general principles are backed up by:

(a) ***data subject rights***: under the Directive, data subjects have rights of access to their personal data, they can require inaccurate personal data to be corrected or deleted, and in limited circumstances they can object to the processing of their data. There is an *absolute* right to object to processing for direct marketing purposes.

  These rights are repeated and expanded in the GDPR.

(b) ***specific rules for specific circumstances***:

  (i) there are more stringent rules on the ***processing of data in particular sensitive categories*** – for example, data regarding race, religion, health or sex life

  (ii) there are restrictions on the use of ***automated processing techniques*** to make significant decisions about individuals which do not involve the exercise of human judgement – for example, in the context of consumer credit screening

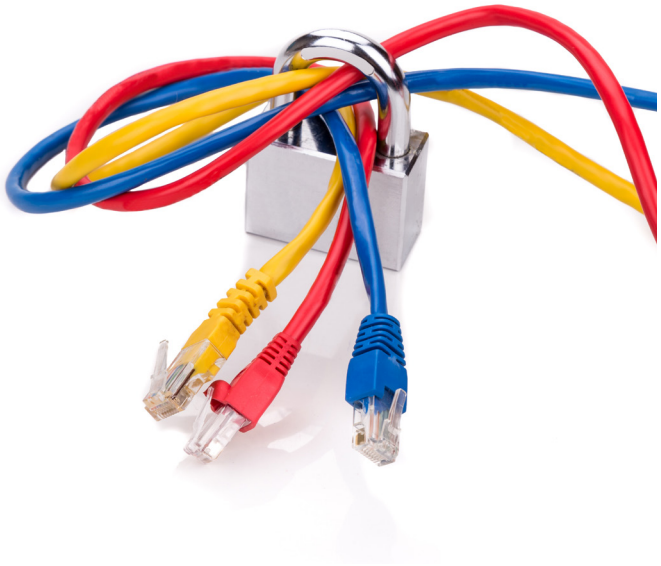
  (iii) there are restrictions on the ***transfer of personal data outside the EEA***, designed to protect data from less stringent foreign data privacy regimes – these transfers can only be made if:

  - the transferred data will be protected by a similarly strict data protection regime (e.g. in Switzerland, or under the "privacy shield" scheme run by the U.S. Department of Commerce)

- steps of various kinds (for example, model form data transfer agreements, approved by the European Commission; or intra-group "*binding corporate rules*") – known as "*adequate safeguards*" – are in place to protect the transferred data
- the data subjects have ***consented*** or one of various other exceptional conditions is met (for example, the transfer is made for important public interest reasons)

(c) ***formal requirements***: controllers are generally obliged to make filings describing their data processing with national data protection authorities, and international transfers based on adequate safeguards sometimes require prior approval.

These formal requirements have proved highly bureaucratic, and will for the most part be abolished by the GDPR.



THE KEY CHANGES – HARMONISATION

The GDPR will take effect on 25 May 2018, replacing the Directive and its implementing laws. In this guide we highlight some of the key changes to be introduced by the GDPR, focusing on:

- substantially increased ***sanctions for breach***
- greater ***harmonisation*** of rules across the EEA
- extension of the regime to regulate ***processors as well as controllers***
- an expansion – but possibly also a contraction – in the effect of the regime ***outside the EEA***
- a series of changes which ***build on the existing data protection principles,*** making them stricter in various respects and introducing new compliance burdens
- the new "***accountability***" requirements

Harmonisation

The GDPR will take direct effect without the need for national implementation. In theory, businesses will now be subject to a consistent data protection regime across the EU and the wider EEA.

The GDPR does, however, leave some room for member states to introduce (or maintain) more specific or different requirements and exceptions in many areas, for example in relation to data about crimes and processing for HR purposes. In practice, there may be quite significant inconsistencies between the national regimes. This remains unclear as the supplemental national laws are unlikely to be finalised until shortly before the GDPR takes effect.

The GDPR also introduces a mechanism, known as the "*one-stop-shop*", regarding supervision and enforcement of its requirements. Broadly, the one-stop-shop provides for a controller or processor established in more than one member state to be regulated – at least with regard to its cross-border processing – by a single "*lead authority*" in the member state where it has its "*main establishment*". The lead authority will be required to coordinate with other authorities as relevant to the supervision of the controller or processor.

The one-stop-shop aims to achieve a more uniform application of EU data protection rules among the data protection authorities. In practice, the success of this mechanism will largely depend on effective cooperation between authorities. It remains to be seen how well this will work. There is still a lot of scope for multiple authorities to seek to regulate the same or similar processing and take different views on the effect of the GDPR.

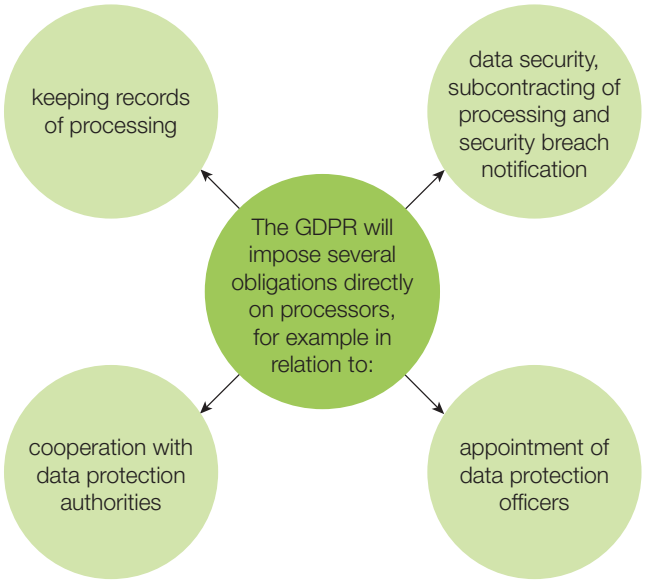
Practical steps

- Businesses will need to consider (i) the extent to which national laws impose more onerous restrictions and obligations, or create inconsistent exceptions to the GDPR regime, and (ii) how to address these restrictions, obligations and inconsistencies in the member states in which they operate
- Businesses should evaluate which data protection authority is likely to be their "lead authority" under the GDPR

Who is regulated?

The current Directive only imposes direct obligations on controllers (entities determining the purposes and means of processing), although the national laws of some member states do directly regulate processors in limited respects (mainly in relation to data security). Generally, processors' obligations are governed by their contracts with their controller-customers.

- The current regime generally only imposes direct obligations on controllers
- Processors (service providers) will be subject to direct obligations under the GDPR



As one would expect, however, controllers will remain solely responsible for compliance with the key data protection principles (other than security, where they will share responsibility with their processors) and the GDPR's international data transfer restrictions, and only controllers will be obliged to respond when data subjects seek to exercise their GDPR rights.

Practical steps

- Processors will for the first time need to consider the direct compliance implications of the data protection regime for their businesses, rather than merely reviewing their customer contracts
- Processors should also consider the impact of the GDPR on their contracts with controllers to ensure appropriate risk allocation
- Identify which arrangements bring your business within the scope of the GDPR as a processor, and those where you act as a controller

THE KEY CHANGES – EXTRA-TERRITORIAL EFFECT/TIGHTENING THE EXISTING RULES

Extra-territorial effect

The GDPR will significantly extend the extra-territorial effect of the EU data protection regime, catching overseas controllers and processors who may have no expectation that they will be caught by EU law. It may also ***reduce*** the regime's extra-territorial effect in one key respect.

The current regime applies:

(a) to processing ***carried out in the context of an establishment of a controller within the EEA***, even if the processing is outsourced to an overseas processor, ***and***

(b) where ***a controller outside the EEA uses equipment in the EEA to process personal data***, including where it appoints a processor within the EEA.

The regime does not generally apply where the controller and the processing are both outside the EEA, even if the data relate to nationals or residents of EEA member states.

The GDPR will also apply to processing entirely outside the EEA if it is carried out ***in order to offer goods and services to, or monitor the behaviour of, individuals within the EEA***. These criteria are not particularly clear – for example, merely allowing individuals within the EEA to purchase goods and services from a website not targeted at them will not be sufficient to fall within the scope of the regime, but there is as yet little indication of what will and will not amount to targeting in this context.

On the other hand, it appears (although this is also not yet clear) that the GDPR may put an end to the application of the EU regime to controllers outside the EEA who outsource their processing to processor-service providers within the EEA. The processors will certainly be bound by the rules applicable to them (for example, they will need to have appropriate security measures in place), but a natural interpretation of the GDPR suggests that their non-EEA customers may fall outside the regime.

Practical steps

- Businesses outside the EEA to consider: do we target offers of goods and services to individuals in the EEA, or monitor their behaviour?
- Global organisations will increasingly need to consider whether to apply standards based on the GDPR worldwide

Tightening the existing rules

The GDPR takes some of the key principles of the current regime and makes them more onerous, including:

Legitimacy of processing/consent

- Obtaining valid consent to data handling will be more difficult. For example, consent will need to be "unambiguous" and clearly distinguished from other terms and conditions
- Individuals can (and must be informed that they can) withdraw their consent at any time

The GDPR preserves the existing principle that all processing of personal data is prohibited unless it meets one of a series of conditions, set out in the law including the consent of the data subject. The conditions themselves will be largely unchanged.

Subtle and important changes are made to the requirements for effective ***consent***, however, and these will force businesses to think more carefully about the basis on which they justify their processing, and review and adjust the mechanisms through which they seek consent.

The GDPR defines "*consent*" as a freely given, specific, informed and unambiguous indication of an individual's wishes. Key changes include:

- **consent must be "*unambiguous*"** (and consent to international transfer must also be "*explicit*"), and, in particular, data protection consents must not be bundled with provisions dealing with other matters
- **while the requirement for consent to be "*informed*" is not new, it will be more difficult to meet** given the GDPR's enhanced requirements on provision of information to data subjects (see below)
- **the need for "freely given" consent is emphasised:**
  - individuals must have a real choice as to whether to consent
  - they can withdraw their consent at any time (and they must be told upfront that their consent can be withdrawn) – mechanisms should be in place to facilitate withdrawal of consent
  - where data are collected as part of the provision of a service, it will rarely be possible to make provision of the service conditional on consent to use of the data for other purposes (for example, marketing)
- it is now clearer that **an active step must be taken to signify consent** – pre-ticked consent boxes, and "opt-out" consents, are unlikely to be effective
- **records must be retained** to demonstrate that consent has been given

There are also new rules on consent from children.

The GDPR confirms the trend in the thinking of EU data protection authorities regarding consent under the current regime. Consent should only be relied upon when processing is genuinely optional – very rarely in the case of employee data, for example – and should then be obtained in a very clear and specific way, with a careful audit trail. In practice, in many circumstances where businesses have in the past relied on – or at least thought that they were relying on – consent, they should under the GDPR justify their processing on the basis of another condition – most likely the need to pursue their own legitimate interests, balanced against any prejudice that the processing may cause to the privacy of the data subjects. This balancing exercise will need to be recorded so that compliance can be demonstrated if challenged.

A factor to take into account in deciding on what basis to justify processing is that personal data processed on the basis of consent will be subject to the GDPR's data portability regime (see below), while data processed on the basis of the legitimate interests condition will not.

"Consent should only be relied upon when processing is genuinely optional."

THE KEY CHANGES – DATA CATEGORIES

Practical steps

- Review circumstances where your business relies on consent to justify processing
- Consider (i) whether consent is still the appropriate basis, and if not (ii) whether another basis – such as "legitimate interests" – might apply
- Amend consent-seeking processes and supporting notices
- Consider seeking refreshed consents, or relying on "legitimate interests" where old consents are no longer valid

"Sensitive" or "special category" data

The Directive tightly regulates processing of personal data in certain particular categories (*race*, *religion*, *political beliefs*, *trade union membership*, *health* and *sex life*) and leaves it to the EU member states to decide how to regulate processing of data relating to criminal offences.

The GDPR will broaden this strict regime to cover data relating to *biometric* or *genetic data* and allow member states to impose even tighter restrictions on the processing of *health, biometric* and *genetic data*.

The approach to *criminal offence data* is also subtly different. The current regime allows member states to impose restrictions but the default position allows data in this category to be processed. The GDPR will prohibit all processing of these data unless it is **specifically allowed** by member state law, opening the possibility of member states failing to deliver sufficiently permissive laws to allow routine and legitimate processing to continue.

Practical steps

- Consider whether your business collects biometric or genetic data
- Ensure compliance with the stricter requirements on the processing of biometric and genetic data (if applicable)
- Be prepared for local rules on health, biometric, genetic and criminal offence data

Providing information to data subjects (transparency)

The GDPR will maintain the principle that, with exceptions (largely unchanged), controllers should give data subjects information about the processing of their personal data and related matters. The GDPR is slightly more explicit than the Directive regarding the need for clear and transparent language in data protection notices, but in this respect it essentially just confirms the law as it is already understood by data protection authorities.

However the GDPR also radically expands the range of mandatory information to be provided, taking away flexibility in cases of relatively routine processing. This is one of the most significant changes in the GDPR, requiring radical redrafting of data privacy statements, policies and terms and conditions across a very wide range of circumstances, affecting almost all

organisations. The expansion is so significant that it will often be necessary to take a new approach to the provision of information, with relatively simple upfront messages backed up by fuller information in linked statements.

Practical steps

- Review and amend notices and policies on informing data subjects
- Consider one-off communications to bring information that you have previously provided up to the GDPR standard

Data security

The GDPR builds on the current regime's data security principle in three key respects:

- as we have already seen, it imposes data security obligations on ***processors as well as controllers***
- it sets much more prescriptive rules as to the ***contractual terms on which controllers appoint processors***
- it introduces a new and very sweeping ***security breach notification*** regime

Appointment of processors

The EU regime requires controllers to satisfy themselves that their appointed processors will keep personal data secure through pre-contract due diligence and appropriate review and audit during the lifetime of the appointment. It also regulates the ***terms on which processors are appointed***.

Under the Directive, a contract between a controller and a processor just needs – broadly speaking – to:

(i) require the processor only to process data on the controller's instructions

(ii) pass on to the processor by contract the controller's legal obligation to have appropriate security measures in place

The GDPR will radically expand the mandatory provisions that must be included in contracts between controllers and processors, dealing in addition with:

- a detailed description of the processing to be carried out
- assistance to the controller with performing various of its GDPR obligations
- restrictions on subcontracting
- information and audit provisions
- return or deletion of data at the end of the arrangement

Processors are also obliged to advise the controller if they think that instructions given to them will result in a breach of the GDPR or other EU or member state data protection rules.

This makes for lengthy, complex and onerous data security provisions, even in contracts where the processing of personal data is an incidental part of a wider service. There is no transitional relief for contracts put in place before the GDPR

THE KEY CHANGES – SECURITY BREACH NOTIFICATION/ PROFILING

takes effect. Furthermore, while the GDPR requires processors to accept more onerous data security terms, the details of which will need to be negotiated (for example, regarding the cost of compliance), processors may also seek additional contractual protection from their controller-customers.

Security breach notification

There is no general "security breach notification" concept under the existing regime. The scope of mandatory reporting requirements is generally limited to telecommunications service providers, although some data protection authorities do encourage voluntary reporting.

The GDPR will introduce mandatory notification requirements in certain circumstances and so significantly alter the EU data security landscape, particularly from the controller's perspective.

Under the GDPR:

- **controllers must:**
  - report security breaches affecting personal data – except for breaches unlikely to give rise to any risk – to their ***data protection authority***
  - inform ***affected data subjects*** of security breaches likely to result in a "high risk" to their "rights and freedoms"
- **processors must** inform their ***controllers*** when they become aware of security breaches affecting personal data

These reports and notices must be given "without undue delay". Where feasible, controllers' reports to their data protection authorities should be made **within 72 hours** of becoming aware of the security breach.

A rapid response to each data security breach will therefore be required: the timer for notifying the authority begins as soon as the controller becomes aware of the data security breach.

Practical steps

- Review security arrangements to ensure compliance
- Build compliance into the contracting process for the engagement of new service providers processing personal data
- Seek amendments to existing contracts under which personal data are processed
- Build consideration of security breach notification obligations into security breach readiness strategy
- Prepare a security breach notification document suite (e.g. including template notification letters to data subjects and regulators).

Profiling/automated decision-taking

The GDPR modifies the Directive's rules on the use of automated decision-taking techniques to make decisions which have legal effect on individuals or otherwise significantly affect them – for example, in the context of credit scoring or screening during recruitment purposes.

Although there has been quite a lot of discussion of the GDPR's profiling provisions, in fact they are closely based on the position as it stands in the current regime. Broadly as in the current regime:

- the use of automated decision-taking techniques to make decisions having legal effects on or otherwise significantly affecting individuals is prohibited unless it is necessary for performing or entering into a contract with the data subject; permitted by a specific local law; or carried out with the explicit consent of the data subject
- appropriate safeguards must be in place (or required by the relevant local law) to protect the data subject

The GDPR:

- expands the scope of profiling activities which might be prohibited, covering processing of data relating to matters such as "personal preferences", "interests", "behaviour" and "location" as well as the narrower categories caught by the Directive ("performance at work, creditworthiness, reliability, conduct", etc.)
- gives some examples of profiling which may have significant effects on individuals (credit and pre-employment screening – but these are examples which would equally be caught by the current regime)
- prohibits processing on the basis of data in the sensitive categories (e.g. health data) except with explicit consent
- as we have seen, makes it more difficult to obtain effective consents or rely on consents obtained under the current regime

The GDPR also explicitly requires data subjects to be informed in advance if they are to be subject to profiling, and given information about the "logic" of the profiling and its likely consequences, but this requirement is implicit in the current regime.

Practical steps

- Identify and review use of profiling / automated decision-taking techniques
- Where possible, avoid reliance on techniques using sensitive data
- Consider legal justification and whether new consents need to be obtained

Data subject rights

The GDPR will substantially expand the rights that individuals can exercise against controllers who are processing their personal data. In particular:

- data subjects' rights to ***object to the processing of their data*** will be strengthened, including express provisions dealing with the "right to be forgotten" already recognised by the EU courts
- there will be a new right of ***data portability***

The rights to object and "be forgotten"

The GDPR provides for a specific and separate "right to be forgotten", allowing data subjects to require their personal data to be deleted. In itself, however, this does not add much to individuals' rights under the existing regime. The right will not arise as long as the controller has a legitimate reason to

THE KEY CHANGES – DATA SUBJECT RIGHTS AND PORTABILITY

continue processing the data, and once that legitimate reason has expired the controller should, in principle, delete or anonymise the data anyway, irrespective of the exercise of the right. In practice, in any case, the European courts have already written the right to be forgotten into the Directive.

More significantly, the GDPR will enhance data subjects' ability to force controllers to cease processing their personal data in circumstances where they do still have legitimate reasons to continue with the processing. This has two components:

- As we have already seen, where controllers are relying on ***consent*** to justify their processing, the consent can be withdrawn at any time, and this must be drawn to the attention of the data subject when they give their consent and facilitated going forward.
- Where controllers rely on "legitimate interests" (or an equivalent "public interest" justification) as the basis for their processing of personal data, data subjects have the right to ***object*** to the processing. Under the current regime, data subjects can only force controllers to cease their processing if they have "compelling legitimate grounds" to object. Under the GDPR the onus will be reversed – a controller will only be able to continue the processing in the face of an objection if it can demonstrate compelling legitimate grounds for the processing which override the data subject's objections.

  This apparently subtle change may have material consequences – the right to object is rarely used under the current regime, because of the need to demonstrate compelling legitimate grounds; it may be used much more frequently under the GDPR, where lodging an obligation places the onus on the controller to demonstrate that it should be allowed to continue. Data subjects can also require the controller to suspend the processing, with potentially disruptive practice consequences, until a final decision is reached.

Practical steps

- Prepare a response package to address data subject objections
- Build a case for all key processing operations which are not "optional" from the data subject's perspective
- Be prepared to deal with objections swiftly

Data portability

The GDPR will introduce an entirely new right of "*data portability*", allowing data subjects to require their personal data to be transferred to them, or passed on to a new replacement controller, in a structured, commonly-used and machine-readable format.

This is not really a data privacy right at all – it is not intended to replace or supplement the existing (and continuing) right of *subject access*, which entitles data subjects to copies of the personal data held about them so that they can check that their privacy is not being infringed. This is more like an ownership right, treating the controller as if it were a processor holding personal data on behalf of the data subject. It is aimed principally at social media and similar online contexts, where providers may consider themselves to be controllers rather than processors because of their contractual freedom to exploit user data for marketing and other

purposes, but users might legitimately regard the data as their own and hope for the right to move them freely between platforms.

Outside these limited contexts the data portability right is potentially alarming – businesses may hold personal data in a wide range of repositories and not be set up to transfer them in a simple package to the data subject; and indeed they may consider the data and their structure to be proprietary to them, not to be passed to and exploited by others. The GDPR does not allow controllers to charge for responding to data portability requests, so in principle the right could lead to substantial and irrecoverable costs for businesses. The right cuts across sector-specific data portability discussions and proposals, which in some sectors (for example in the UK banking sector) are relatively well-developed.

The GDPR does limit the exercise of the right in two key respects, which may in principle mean that it is not widely used:

- the right only applies to personal data ***provided to the controller by the data subject*** – not to data which the controller has created itself or obtained from third-party sources – although it appears that the concept of provision by the data subject will be interpreted rather broadly
- the right only arises where processing of the data is justified on the basis of ***consent***, or because it is ***necessary for performance of a contract with the data subject*** – it does not arise, for example, where processing is justified based on "legitimate interests"

"This is not really a data privacy right at all – it is not intended to replace or supplement the existing (and continuing) right of *subject access*, which entitles data subjects to copies of the personal data held about them so that they can check that their privacy is not being infringed."

Practical steps

- Consider circumstances in which the portability right may be used against your business and, where portability would not be appropriate, how it can be avoided (for example, by relying on "legitimate interests" rather than "consent" to justify processing)
- Where relevant, review systems and develop compliance plans to facilitate a low-cost response to portability requests

International data transfers

The GDPR substantially preserves the current international data transfer regime. There are, however, some significant changes:

- While it will still be possible to transfer personal data to countries outside the EEA which ensure "adequate" protection for personal data, the GDPR will not allow an exporting controller to reach its own view on the adequacy or otherwise of a country's data protection regime. Unless the relevant country is on the European

THE KEY CHANGES – INTERNATIONAL DATA TRANSFERS/ ACCOUNTABILITY

Commission's list of approved countries, it will be assumed not to be adequate. This may not be a major change in practice as businesses have over the years become increasingly cautious about reaching their own views on adequacy in relation to particular data transfers. In this respect, in any case, the GDPR position is already written into the law – or into how the law is understood – in some member states (e.g. France).

- There are changes to the basis on which exporting controllers can rely on adducing "adequate safeguards" for transferred personal data to justify international transfers:
  - the "binding corporate rules" scheme, through which intragroup transfers can be approved on a pan-EU basis, will now be built into the regime, with an amended (and possibly simplified) approval mechanism. It remains to be seen whether this will make the scheme any more attractive. There has been low take-up to date, and the very substantial resources and effort required to obtain an approval will still need to be taken into account
  - on the other hand, where a transfer is justified by putting in place a data transfer agreement in one of the European Commission's standard forms, member states will no longer be able to insist on the transfer and/or the agreement being pre-approved by the national data protection authority, with associated delays and – in some member states – difficult formal requirements and objections. In practice, this may lead to even greater reliance on standard form agreements, rather than on binding corporate rules which will still require approval

International transfer strategies may also be affected by the changes to the ***consent*** regime discussed above. It will be difficult under the GDPR to justify transfers of personal data outside the EEA on the basis of consent except in rather limited, one-off contexts where all the requirements for an explicit consent can be met. The GDPR does introduce a new "*legitimate interests*" condition allowing transfers to inadequate countries without consent, but it is so narrow, and subject to such difficult associated requirements (for example, to notify data protection authorities on a transfer-by-transfer basis) that it is likely to be relied upon only in very rare circumstances. The other conditions for transfer to inadequate countries are essentially unchanged.

Practical steps

- Review approach to international data transfer to ensure compliance with current regime and that it does not rely on the firm's own assessment of the adequacy of a third country's data protection regime
- Ensure a systematic review process is in place to check that each international data transfer is covered by a GDPR-compliant transfer mechanism

"It will be difficult under the GDPR to justify transfers of personal data outside the EEA on the basis of consent except in rather limited, one-off contexts where all the requirements for an explicit consent can be met."

Accountability

The GDPR will introduce a series of new "accountability" principles, intended to encourage businesses to take data protection seriously and build it into their processes and systems, and to improve compliance with the regime's essentially unchanging data protection principles.

The new rules place an onus on businesses to understand how their processing activities pose risks for individuals, and require them to protect individuals from these risks. They require them to be able to **demonstrate** how the GDPR has been complied with. They place the burden of proving compliance firmly on controllers and processors.

The key accountability principles include:

Keeping records of processing

Under the existing regime controllers are required, with exceptions, to notify data protection authorities before processing personal data. Controllers maintain filings with the authorities describing their processing of personal data. The regime is established on a country-by-country, controller-by-controller basis, and varies considerably between member states.

The GDPR replaces these requirements with a requirement to keep internal records of all processing activities, including certain specified details (e.g. the purposes of the processing and a general description of the security measures in place). The requirement extends to processors as well as controllers.

Controllers, at least, may welcome this reduction in their regulatory burden. Audits of processing activities will be necessary for the preparation of these processing records but would, in any case, be essential so that businesses can put themselves in a position to demonstrate compliance with the GDPR generally.

Businesses should consider the appropriate type of audit (from very detailed to light-touch, depending on the nature of the organisation).

Practical steps

- Audit of processing arrangements
- Regular refresh of audit

Demonstrating compliance

The GDPR will specifically require records to be kept to allow controllers to demonstrate that they have collected appropriate consents where they rely on consent to justify the processing or international transfer of personal data. More widely, it will require appropriate measures to be in place to be able to demonstrate compliance with all of the GDPR requirements.

Careful consideration will need to be given to the scope of these requirements and, in particular, to how granular a business should be in considering its processing operations and being in a position to demonstrate compliance.
A combination of policies and guidance, communications and training, record-keeping systems and audit will be necessary, with the balance between the various components closely dependent on the nature of the business.

Practical steps

- Build a compliance infrastructure of policies and guidance to encourage compliance
- Communicate compliance strategy, with associated training
- Build mechanisms to demonstrate compliance (e.g. record consents, record decisions as to other processing)
- Carry out regular audits of compliance with the GDPR rules

THE KEY CHANGES – PRIVACY BY DESIGN

Privacy by design

The new rules require businesses to build privacy – and, in particular, a focus on proportionality and the anonymisation or pseudonymisation of data – into the design of their processing activities.

Appropriate measures to implement data protection principles should be considered at the outset of each new processing arrangement. Current arrangements may need to be redesigned to fit the new requirements. Data protection impact assessments (discussed below) will be an important element of assessing whether a controller's privacy framework is adequately designed to comply with the GDPR.

A user-centric approach to minimising the personal data required to carry out a business's processing activities will contribute to building a healthy privacy compliance architecture. For example, ensuring that systems only require minimal personal data to carry out their functions (e.g. default settings requiring approval for the provision of data in new categories).

It will be important to maintain a record of compliance decisions and document how the business has thought through how the new rules will be designed into (and throughout) its business framework.

Practical steps

- Build the new rules into policies governing the development and procurement of new systems and processes

Data protection impact assessment

The GDPR will require controllers to carry out "*data protection impact assessments*" before carrying out any data processing which:

(a) involves new technology ***and***

(b) is likely to be of high risk to data subjects.

The scope of this requirement is not yet clear – it will be the subject of regulatory guidance, currently in draft – but, in practice, basic assessments will be needed of *all* processing arrangements to ensure that they comply with the substantive requirements of the GDPR and to determine whether full assessments are necessary. A full assessment will involve review of the proposed processing arrangements, all the associated risks to privacy and the steps that can be taken to address those risks. A record will need to be made of each assessment and its conclusions.

Where a data protection impact assessment concludes that any data processing might result in a high risk to individuals which is not appropriately mitigated by the compliance steps to be taken, the controller must consult with the relevant data protection authority. The circumstances where consultation is required are, as yet, unclear. The authorities are unlikely to have the resources to review huge numbers of applications for approval.

It appears, although it is not yet clear, that full data protection impact assessments will not be mandatory in the case of systems already in place when the GDPR takes effect. All systems will, however, need to be reviewed in a less formal way to ensure compliance.

Practical steps

- Establish a data privacy impact assessment framework
- Build data protection impact assessments into the procurement of new systems as a general compliance requirement
- Maintain records of each data protection impact assessment (to ensure that authorities can trace your risk assessment on a step-by-step basis)

Appointment/role of data protection officer

Private sector controllers and processors processing sensitive data on a large scale, or whose core activities require regular and systematic monitoring of data subjects on a large scale, and practically all public authorities, will have to appoint data protection officers (DPOs). Member states can also opt to require other organisations to appoint DPOs – it is likely that Germany, for example, will continue with its current model, where the appointment of DPOs is mandatory even for relatively small organisations.

There are complex rules on the role of the DPO. They will have to be closely involved in all issues relating to the processing of personal data, to report directly to the highest management level of the business, and to be protected from dismissal or other reprisal resulting from their decisions. Unless carefully crafted, the role could prove to be an uncomfortable mixture between a data protection adviser to the business and a kind of internal data protection authority.

Practical steps

- Consider whether the business' core activities involve (i) processing "sensitive" data on a large scale, or (ii) regular and systematic monitoring of data subjects on a large scale
- Appoint a DPO (if required)
- Appointing a DPO is just the first step – ensure (i) sufficient budget is available to support the DPO, and (ii) staff are trained and aware of the DPO's responsibilities

Guidance and local law

- A working party of representatives of the European data protection authorities, established under article 29 of the Directive, is producing guidance on various aspects of the GDPR
- The working party has so far published guidance, or draft guidance, on ***the one-stop shop mechanism, data portability, data protection officers*** and ***data protection impact assessments***
- Further working party guidance is expected on ***data protection certification schemes, administrative fines, consent and profiling, transparency, international data transfers*** and ***breach notification***
- A raft of complex new laws will be required at the member state level to supplement and create exceptions to the GDPR principles

THE INTERNATIONAL IMPACT OF THE GDPR

Extra-territorial Effect

If the controller or processor is established outside the EU and either:
(i) offers products or services to individuals within the EU; (ii) or monitors the behaviour of individuals, it will be subject to the GDPR and to the scrutiny of each relevant regulator.

On the other hand, a controller outside the EEA may no longer be subject to the regime just because it uses a processor within the EU.

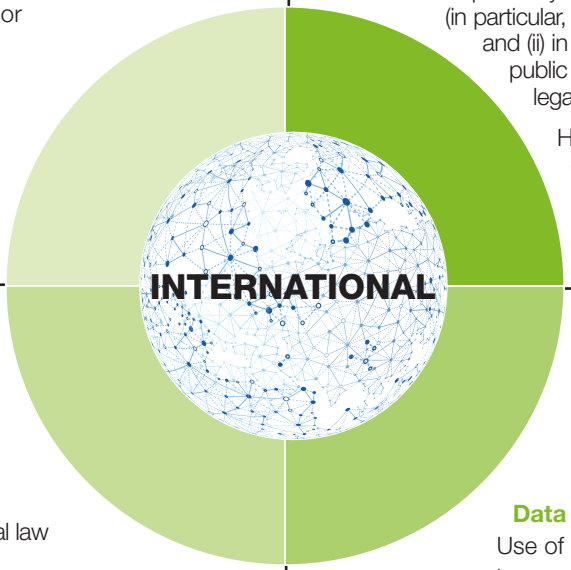
"One-Stop-Shop"

The GDPR has introduced a consistency mechanism (i.e. to simplify the regulation of privacy-related matters across member states). Legal entities/businesses will, in theory, be regulated by a single lead regulator. The relevant single lead regulator will be the regulator in the place in which the legal entity has its "main establishment".*

* Various considerations will define what constitutes "establishment" – the test is broad. In practice, relevant considerations will include (i) whether the relevant entity conducts any real and effective activity in the EU, and (ii) whether the entities main administrative location in the EU.

Local supervisory authorities will continue to play a role (in particular, (i) in cooperating with the lead regulator; and (ii) in regulation processing carried out for public interest purposes/in connection with legal obligations).

However, the provisions of the GDPR do not clearly set out how this consistency mechanism will work in practice; and concerns exist in relation to forum shopping.



Regulation not Directive

Significantly, in contrast to the previous European regime, the new regime will be implemented by way of a ***regulation***. This will lead to a greater level of harmonisation as it will take effect without needing to be transposed into the national law of each member state.

Despite this, there remains a wide scope for local variation. For example, the GDPR:
(i) permits member states to make exceptions to the GDPR requirements on various grounds (broadly mirroring the Directive); (ii) permits different laws on processing of employee data; and (iii) depends in various respects on concepts being recognised in EU or member state law.

Data Transfer Restrictions

Use of standard contractual clauses will no longer require the prior approval of a data protection authority (the existing position in many member states).

Data controllers intending to export personal data can no longer make their own independent assessment of the adequacy of the level of protection of the importing countries.

THE IMPACT OF BREXIT

The GDPR will almost certainly take effect before the UK leaves the EU, which is unlikely to be before March 2019. UK businesses will therefore need to comply with the GDPR in full, at least during the period between May 2018 and Brexit.

Since the GDPR is an EU Regulation, rather than a Directive implemented in UK national law, it will cease to have effect in the UK on Brexit. In practice, however, it is likely that the GDPR will immediately be replaced in the UK by a new law having essentially the same substantive effect, with only the minimum changes necessary to reflect the fact that the UK is no longer an EU member state (for example, the arrangements through which the European Commission assesses the adequacy of the data protection laws of countries outside the EU will presumably be replaced by similar arrangements in the hands of a UK authority). In the longer term, the UK may opt to depart from the EU data protection model, but that is entirely unpredictable at this stage.

Although UK law post-Brexit is likely to be closely based on the GDPR, this does not mean that Brexit will be unproblematic from a data protection standpoint. All being equal, the post-Brexit UK will be regarded by the EU as an 'inadequate' country for data transfer purposes until (if ever) the European Commission determines that UK law ensures an adequate level of protection for EU personal data. Unless a special exception is agreed, transfers of personal data from the EU to the UK will therefore be prohibited, at least for an initial period, except where the GDPR allows transfers to 'inadequate' countries. The process of reaching an adequacy determination may take some time. Indeed, it may be difficult to reach in practice given, for example, the UK's legal position on state access to private communications. Transfers from the UK to the EU may, in principle, raise a similar issue.

Unless a transitional or permanent solution to these problems is found through the Brexit negotiations, businesses will need to find alternative means (most likely standard form data transfer agreements or binding corporate rules) to justify data sharing between the EU and the UK in future.

Practical steps

- Businesses should be taking Brexit into account in assessing their international data transfer strategies in readiness for GDPR
- Review the terms on which your business outsources processing to processors through arrangements which may include movements of personal data between the UK and the EU

GDPR
COMPLIANCE CHECKLIST

Many issues will arise from the GDPR. Focusing attention on key pressure points which strategically affect your business will be important now, particularly as the implementation deadline rapidly approaches. The following checklist offers a targeted, conceptual list pointing towards key areas to consider now, and draws together the more comprehensive practical steps considered earlier in this guide.

1. Does the GDPR apply?	
(a) Consider whether your business is likely to come within the GDPR's scope (particularly non-EEA businesses)	☐
(b) Identify specific arrangements which may bring your business within the GDPR's scope (either as controller or processor)	☐
(c) Undertake cost and risk analyses for compliance with the new rules	☐
2. Accountability	
(a) Carry out data privacy impact assessment (i.e. to isolate "high-risk" data processing activities)	☐
(b) Review security arrangements for new and existing technological infrastructure now (e.g. document sharing sites and email servers), including review of security breach readiness/notification strategy	☐
(c) Analyse whether a DPO will be required under the rules. If yes, appoint one	☐
(d) Review and amend data protection policies to meet the GDPR standards	☐
(e) Deliver high-level training to key staff involved in the processing of personal data (i.e. in light of the new rules)	☐
(f) Consider complying with an industry code of practice – if there is one – to demonstrate compliance	☐
3. Justification Strategy	
(a) Review the organisation's strategy for the justification of its processing of personal data in light of the new regime (particularly with regard to consent)	☐
(b) Where consent is still to be relied upon, redesign forms of consent and consider refreshing consents obtained under the old regime	☐
4. Record-Keeping, Data Privacy Assessments and Documentary Requirements	
(a) Apply initial data protection impact assessment process to each of the business' systems and processes (i.e. to determine whether a full impact assessment is required)	☐
(b) Prepare a compliance questionnaire (multi-jurisdictional, if applicable) to support data processing auditing/assessment processes	☐
(c) Provide for regular audit cycles to identify material changes in data privacy laws (e.g. proposed ePrivacy Regulation, if implemented)	☐
(d) Document the result of audits/data privacy assessments (e.g. to assist with future interaction with data protection authorities)	☐

5. Transparency	
(a) Address transparency in data protection policies (e.g. regarding information included in respect of data collection processes)	☐
(b) Review and amend notices and policies on informing data subjects	☐
(c) Prepare standard notice to employees and contractors (e.g. for inclusion in documentation regarding processing of their personal data)	☐
(d) Consider one-off notifications to "refresh" notices given under the old regime	☐
6. Outsourcing Management	
(a) Identify key existing contracts which will extend significantly beyond 25 May 2018 and involve material outsourced processing of personal data	☐
(b) Review existing processing contracts – renegotiate terms to ensure GDPR compliance, if necessary	☐
(c) Incorporate GDPR – compliant provisions in new contracts	☐
(d) Prepare GDPR compliance checklist, drawing on standard terms, for use in review of contract terms proposed by potential service providers	☐
7. International Data Transfers	
(a) Review approach to international data transfers – ensure that cross-border data transfers are not reliant on the business's own assessment of the "adequacy" of a third country's data protection regime	☐
(b) Identify key processes and systems involving restricted intra (or extra-) group international transfers of personal data	☐
8. Data Subject Rights	
(a) Consider extent to which new consent rules will impact your business (e.g. are your data processing arrangements heavily reliant on existing consents?)	☐
(b) Analyse requirements (technological, legal and practical) arising in connection with new data subject rights (e.g. maintaining the ability to "port" data to third parties)	☐
(c) Prepare a response package to address exercise of data subject rights	☐
9. Brexit	
(a) Consider impact of Brexit in assessing international data transfer strategies	☐
(b) Review the terms on which your business outsources processing to processors (in particular, where the arrangements include movements of personal data between the UK and other EU member states)	☐
10. Local and Parallel Data Privacy Laws	
(a) Keep national laws supplementing and creating exceptions to the GDPR under review and, where necessary, devise local compliance strategies	☐
(b) Analyse applicability of NIS Directive to your business (i.e. in parallel with GDPR analysis)	☐
(c) Analyse applicability of the current ePrivacy Directive and potential ePrivacy Regulation to your business	☐
(d) Consider implications of potential parallel security breach notifications under the three data privacy regimes	☐

HOW CAN WE HELP?

We advise on a wide range of data privacy and related M&A, outsourcing and regulatory projects.

At a high level, we can help to guarantee the success of the GDPR compliance project through:

Gap analysis of your current compliance regime vs future requirements

Strategic discussion and guidance

- long-term strategy to address "legitimacy" (e.g. consent/transparency issues)
- international data transfer strategy
- ongoing compliance infrastructure (audit, privacy impact assessment, etc.)

Construction and review of "legal" project deliverables

- enhanced privacy policies
- privacy impact assessment toolkits, including data capture forms
- customer/supplier/employee/website consents and notices
- standard data security terms for the use of third-party processors
- security incident response plans
- framework intra-group data transfer agreements and external transfer templates

help with "what are other firms doing?" and industry insight questions

local law advice as the EU member states supplement, and make exceptions to, the GDPR

high-level consciousness raising and preparation of internal training materials

CONTACTS

Jonathan Kewley
Partner
London
T: +44 20 7006 3629
E: jonathan.kewley@cliffordchance.com

Richard Jones
Director of Data Privacy
London
T: +44 20 7006 8238
E: richard.jones@cliffordchance.com

André Duminy
Partner
London
T: +44 20 7006 8121
E: andre.duminy@cliffordchance.com

Dessislava Savova
Partner
Paris
T: +33 14405 5483
E: dessislava.savova@cliffordchance.com

Megan Gordon
Partner
Washington
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com

Alexander Anichkin
Partner
Moscow
T: +7 495258 5089
E: alexander.anichkin@cliffordchance.com

Alvin Khodabaks
Partner
Amsterdam
T: +31 20711 9374
E: alvin.khodabaks@cliffordchance.com

Susanne Werry
Senior Associate
Frankfurt
T: +49 697199 1291
E: susanne.schuler@cliffordchance.com

Tim Grave
Partner
Sydney
T: +61 28922 8028
E: tim.grave@cliffordchance.com

Natsuko Sugihara
Partner
Tokyo
T: +81 3 6632 6681
E: natsuko.sugihara@cliffordchance.com

Luna Hiraoka
Senior Associate
Tokyo
T: +81 3 6632 6327
E: luna.hiraoka@cliffordchance.com

Lena Ng
Partner
Singapore
T: +65 6410 2215
E: lena.ng@cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

WWW.CLIFFORDCHANCE.COM

J20172104170102