WAVESTONE

IMPACT OF THE NEW GDPR DIRECTIVE ON OUTSOURCING ARRANGEMENTS

This Insight provides an overview of the changes, and impact the GDPR Directive presents to outsourcing arrangements. Furthermore, it provides a high-level view of some of the key steps companies and service providers should be taking to address and mitigate the impact prior to the effective date in May 2018.

AUTHOR

MARK GIBBONS
mark.gibbons@wavestone.com

The notion of privacy rights has been around for some time with its origins tracing back to the 'Universal Declaration of Human Rights' in 1948. However, it was only in the early 1970s, that countries began adopting broad laws intended to protect individual's privacy rights, and subsequently a general movement towards the adoption of comprehensive privacy laws that set a framework for protection. The most comprehensive step came with the EU Data Protection Directive in 1995 and implemented in the U.K. in 1998.

However, since 1998 there has been a rapid explosion of new data driven technologies, which has seen individuals more likely to freely provide personal and often sensitive data to third parties and their applications more willingly; and companies and employers adopting more integrated technology solutions and data mining practises in a more thorough way than ever before.

As a result, it soon became apparent that the existing EU Directive was no longer fit for purpose. The GDPR was conceived to take a broader and deeper approach to protecting individuals' data within the digital era. This means that any company that works with information relating to EU citizens will have to comply with the requirements of the GDPR, making it the first truly global data protection law standard.

This substantial shift presents several challenges for companies and service providers.

The good news for most organisations, is that the EU Directive will have laid the foundations for GDPR as policies, procedures, and processes are already in place. Most contractual provisions in modern outsourcing arrangements will have extensive provisions incorporated for the protection of data and there will typically be internal controls and governance frameworks already in place, as well as senior management oversight.

But there are some fundamental changes!

This Insight provides an overview of the changes and impact the GDPR presents to outsourcing arrangements and moreover provides a high-level view of some of the key steps companies and service providers should be taking to address and mitigate the impact prior to D-day in May 2018.

WHAT ARE THE KEY CHANGES?

If the EU Directive was a step in the right direction, then the GDPR makes a giant leap. There are a series of new rules, enhanced individual rights, and the concept of "data privacy by design". The following diagram highlights the top ten changes:

Let's take a look at each of these changes in more detail:

1. **Extra territorial measures:** The GDPR expands the territorial and material scope of EU data protection law. It applies to both Controllers and Processors established in the EU, and those outside the EU who offer goods or services to, or monitor, EU citizens' data.

2. **Sanctions:** The GDPR provides wide-ranging powers to enforce compliance, including the power to impose significant fines. You will face fines of up to €20m or 4% of your total worldwide annual turnover of the preceding financial year.

3. **International transfers:** Much like the EU Directive the GDPR allows for international data transfers to countries outside the EEA where the country securing the personal data provides for an "adequate" level of protection. Transfers of personal data within the EEA will continue to be allowed.

   The European Commission has the power to decide if a country outside the EEA provides adequate protection and declare "a territory or one or more specified sectors within that country" adequate.
   For example, although the United States is not deemed to be an "adequate" jurisdiction, as of 1 August 2016, organisations located in the U.S. may register with the EU-U.S. Privacy Shield.

   The GDPR recognises several tools for international data transfers to countries outside the EEA, including:

   - Binding corporate rules, which require the approval of the national data protection authorities [Binding Corporate Rules («BCR») are internal rules (such as a Code of Conduct) adopted by multinational group of companies which define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection – focus is provide clarity where there are local differences]
   - Standard data protection clauses, also called standard contractual clauses (SCCs). These will replace the Model Contract Clauses under the EU Directive
   - An approved code of conduct or an approved certification mechanism with binding and enforceable commitments of the organization receiving the personal data in the country outside the EEA.
   - EU/US Privacy Shield.

4. **"One-Stop Shop" concept:** The one-stop shop is the name for a new cross-border data protection regulatory regime for the EU. It means that data controllers are regulated by a lead data protection authority located in the territory of their main establishment.

5 **Data Processors:** The GDPR imposes direct statutory obligations on Data Processors, which means they will be subject to direct enforcement by supervisory authorities, fines, and compensation claims by data subjects. The changes expand the mandatory terms which must be included in processing contracts

6 **Accountability Principle:** The GDPR introduces a new concept of accountability, which requires you to be able to demonstrate how you comply with the GDPR. Under this principle, the data controller is responsible for, and must be able to demonstrate, compliance with the data protection principles. Accountability therefore includes obligations such as implementing appropriate technical and organizational measures, to keep records of processing activities, and to carry out Privacy Impact Assessments, among other requirements.

7 **Consents:** The GDPR sets out stricter rules - consent must be freely given, specific, informed and unambiguous. Whilst built on the same principles as the definition of consent in the EU Directive, the GDPR provides clarity as to what constitutes valid consent. Individuals should indicate their wishes either by a statement or clear affirmative action. Organisations can no longer rely on implied consent. In principle, individuals need to be provided with information regarding the collection and further processing of their personal data before the data controller starts processing it.

Also note, Data subjects can withdraw their consent at any time, and it must be easy for them to do so.

8 **Individual's rights:** Some new and some are enhanced rights, including:

- right to data portability: (which allows individuals to obtain and reuse their personal data for their own purposes across different services)
- right to erasure (aka: right to be forgotten): which is a broad principle to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- right not to be subject to a decision based on profiling: for example, the right to opt out/unsubscribe from profiling. Profiling is defined as an automated processing of personal data, which is used to evaluate personal aspects of an individual whenever there is prediction or analysis of an individual's personal aspects. For example, the use of an algorithm for analysing data to assess an individual's or a category of individuals' interests in a certain type of products or services, the likelihood for an individual to purchase a certain product, to behave in a certain way, or to be at a certain location, most likely qualifies as profiling.

9 **Security and breach notification:** If you are a Controller, you will have a mandatory obligation to notify your supervisory authority of a data breach within 72 hours.

The approach of the GDPR to security is linked to the new obligations to ensure that privacy is considered at the very start of projects (i.e. privacy by design), to ensure that privacy settings are designed to block contact (aka "privacy by default") and to ensure that assessments are made of the impact of new projects on individuals' privacy rights (Privacy Impact Assessments).

10 **Privacy notices:** The GDPR increases the amount of information that you must provide to data subjects when collecting their personal data, to ensure that your processing activities are fair and transparent.

WHAT IS THE GDPR'S LIKELYS IMPACT ON OUTSOURCING CONTRACTS?

Although many outsourcing arrangements will have already adopted privacy processes and procedures consistent with the Directive as a normal industry practice the changes mentioned above are far more extensive and wide-ranging when compared to the outgoing regime.

With the GDPR Directive coming into effect in May 2018, organisations should have conducted an impact assessment by now to understand the risk to the organisation and be moving onto implementation mode.

Wavestone advises its clients that the assessment is the easy task (relative to the organisation's own data protection maturity) but the real challenge is the implementation of change!

There are many variations of outsourcing arrangements, but in this Insight we focus two key areas: Contractor / Processor arrangement; and their application to IT Infrastructure arrangements.

HOW DO THE CONTRACTOR / PROCESSOR ARRANGEMENTS AFFECT OUTSOURCE ARRANGEMENTS?

The net result, is that the GDPR changes will likely alter the contractual relationship between Data Controllers and service providers acting as Processors.

For example, article 28 of the GDPR provides a lengthy list of obligations that the Controller will need to impose on the Processor which is a significant extension from the current Directive, and as we have seen the sanction risks associated with non-compliance far greater than ever before. Such clauses to be covered off in a data processing contracts may be classified into three areas:

- Clauses which impose technical and organisational measures on the processor;
- Clauses which increase the communication/cooperation between the controller and the processor;
- Clauses which allocate the risk of non-compliance in the performance of the contract between the parties.

However, it is important to note that the compliance risk will weigh on both the data controller and the processor respectively which will require more focus in the contract to protecting each other's liability.

Accordingly, the GDPR's more detailed requirements for Controller-Processor contracts may compel some data controllers to reassess their third party outsource agreements to achieve compliance. Processors not only have additional duties under the GDPR, moreover, they also face enhanced liability for non-compliance or for acting outside the authority granted by a controller. Such detailed requirements and the delineation of responsibility between the Controller and the Processor will likely be subject to far more detailed contract negotiations about data protection than ever before. Nonetheless, the burden for personal data protection under the GDPR still rests primarily with controllers.

OVERARCHING CONCERNS OF EXISTING OUTSOURCING CONTRACTS

From the viewpoints of both Controller and Processor, it means navigating a sea of contractual provisions, reviewing, updating or re-drafting current outsourcing contracts and, sometimes, more drastically re-thinking the business / operating model that's currently in place. This may involve raising change control requests for changes to be agreed and incorporated into the existing arrangement or entering into a new contract altogether where the scope of change is significant, or the existing arrangement is no longer fit for purpose in a post-GDPR world.

Now is the time to review and adapt existing outsourcing contracts to the new requirements. But the complexity will be around the BAU operational environment ensuring that there are processes, systems and tools in place from May onwards to meet the new obligations.

To determine if GDPR affects your organisation, there are some back-to-basics questions to ask yourself, such as:

- Are you a Controller?
- Are you a Processor?
- Do you offer goods and services to EU residents?
- Do you rely on third parties that store or transmit data to or from the EU?
- Do you collect, transmit or process data pertaining to EU residents?

It doesn't matter if the services are free and as mentioned earlier the changes to extra-territorial reach means that it also doesn't matter whether your company operates in the EU or not.

However, it will be important for all organisations to understand where they fall within the GDPR. This becomes more complicated for some modern technology solution providers (such as cloud services, digital working solution providers).

The concerns for both **the Controller and the Processor** are:

- reviewing the existing data processing contracts,
- assessing whether amendment is needed or not,
- regularly checking for further guidance from EU and national authorities.

The key concerns of **the Controller** only are: assessing the ability of current contracting Processors to comply with the GDPR. If it is not the case, contracts with these parties should not be renewed. When assessing the value of a processing service, controllers cannot focus solely on the cost anymore.

They must also consider the capacity of the service to perform the contract in accordance with the GDPR. For example, this capacity can be demonstrated by the participation of the processor in a certification programme approved by supervisory authorities or the adoption by the processor of a code of conduct.

The key concerns of the **Processor** only are:

- now that Processors are in-scope it is more important to analyse its new obligations under the GDPR,
- verifying that procedures to identify, assess and promptly report data breaches to the controller are in place,
- reviewing the existing sub-processing contracts and identifying what needs to change or the potential impact,
- assessing whether participating in a data protection certification or adopting an approved code of conduct is necessary or not.

The key concerns for the Controller and the Processor are displayed graphically in the following diagram:

Service providers acting as Processors will be at risk of fines going forward and, in addition, the maximum fine for some breaches will increase to EUR 20 million or 4% of annual worldwide turnover in the previous year, whichever is higher. This is significantly higher than the current maximum penalty in the UK of £500,000.

For **IT infrastructure providers**, there is potential of applicability to certain infrastructure solutions which may not have traditionally fallen within the remit of a "Processor". For example, Cloud infrastructure solutions could potentially be at odds with the GDPR. Service providers will need to understand what the impact and risk of the GDPR will presents to their existing solutions as well as future product and solution design and development where personal data is involved. Laws drafted for old outsourcing models just won't work for commoditized, standardized, pre-built, self-service public cloud, particularly infrastructure cloud, and other modern outsourcing models/ solutions. Under the GDPR, infrastructure cloud providers may potentially fall in line as "processors"; whereas equipment manufacturers/ vendors may not. Individuals and organisations that rely on infrastructure cloud services for computing, storage and networking purposes instead of buying their own equipment may be impacted the most. For example, the providers of cloud infrastructure services (i.e., IaaS/PaaS or SaaS) may be considered "processors" which in turn may mean clients revisiting their cloud use.

GDPR places **Restrictions on Sub-Contracting** through GDPR Articles 26(1a), 26(2)(d) which require controllers' prior consent to sub-processors who are "enlisted" by processors. This could mean that cloud providers where services are already built on a sub-providers' pre-existing service (i.e.: Dropbox's SaaS storage on Amazon's IaaS) may mean that the customer must either consent, or not use that provider's service to be within the scope of the GDPR. It will be difficult for service providers to mitigate this risk as for the time being it is unlikely that they will be able re-design their services to work with any sub-provider's service just because one prospective customer objects to a sub-provider having access to their data.

FOR BOTH THE CONTROLLER AND THE PROCESSOR:

- Reviewing the existing data processing contracts,
- Assessing whether amendments are needed or not,
- Regularly checking and updating policies & procedures.

FOR THE CONTROLLER ONLY:

- Assessing the ability of current contracting. Processors to comply with the GDPR,
- Reviewing the technical and functional scope of the service to perform the contract in accordance with GDPR.

FOR THE PROCESSOR:

- Analysing its new obligations under the GDPR,
- Verifying procedures to identify, assess and report data breaches to the Controller are in place,
- Reviewing the existing sub-processing contracts and identifying what needs to change or the potential impact,
- Determining whether a data protection certification or adopting an approved code of conduct is required.

If cloud providers are potentially "processors", their infrastructural sub-providers may potentially be considered as sub-processors, i.e. data centre operators and connectivity or network service providers. This problem goes beyond cloud. Imagine asking every third-party data centre operator and carrier involved in a technology service's delivery to sign a contract on Article 26(2)'s prescriptive terms for every customer who processes personal data using that service – cloud or not. Thousands of tailored contracts for every service involving personal data processing (cloud or not) is impracticable and doesn't necessarily help data protection.

IN CONCLUSION

Laws drafted for old outsourcing models just won't work for commoditized, standardized, pre-built, self-service public cloud, particularly infrastructure cloud, and other modern outsourcing models.

In the short term this will most likely mean that contracts will need to pay greater care and attention to the GDPR principles through an additional focus on designing privacy into every aspect of a sourcing project from start to contract signature.

From a pure contractual perspective this will mean a heavy focus on contracting for customer disclosures, representations, warranties and indemnities, which may increase costs and potentially reduce performance. It is likely the risk burden for both sides will increase and need to be priced into the contract.

There will also be a greater degree of "flow-down" of protection within the service providers supply chain especially where sub-processors are enlisted for a "specific processing," but the full meaning remains insufficiently clear. One consequence (presumably unintended) of the GPDR is that only large customers and providers are likely to have the resources and bargaining power to make the entire supply chain sign the detailed, prescriptive (and cloud-inappropriate) contracts that Article 26 would require. Small customers and providers will be unable to operate – or may choose not to comply, despite potentially huge fines, taking the risk that regulators with limited resources will not go after a "small fry." But that would bring the GDPR into disrespect.

There's no "grandfathering" of pre-existing contracts that comply with current EU Data Protection Directive requirements. With contracts expiring after the GDPR

takes effect, change control or change of law clauses will need to be included now, so that they can be amended to comply with GDPR Article 26 (as well as to allocate responsibility among supply chain actors with appropriate liability/indemnity clauses).

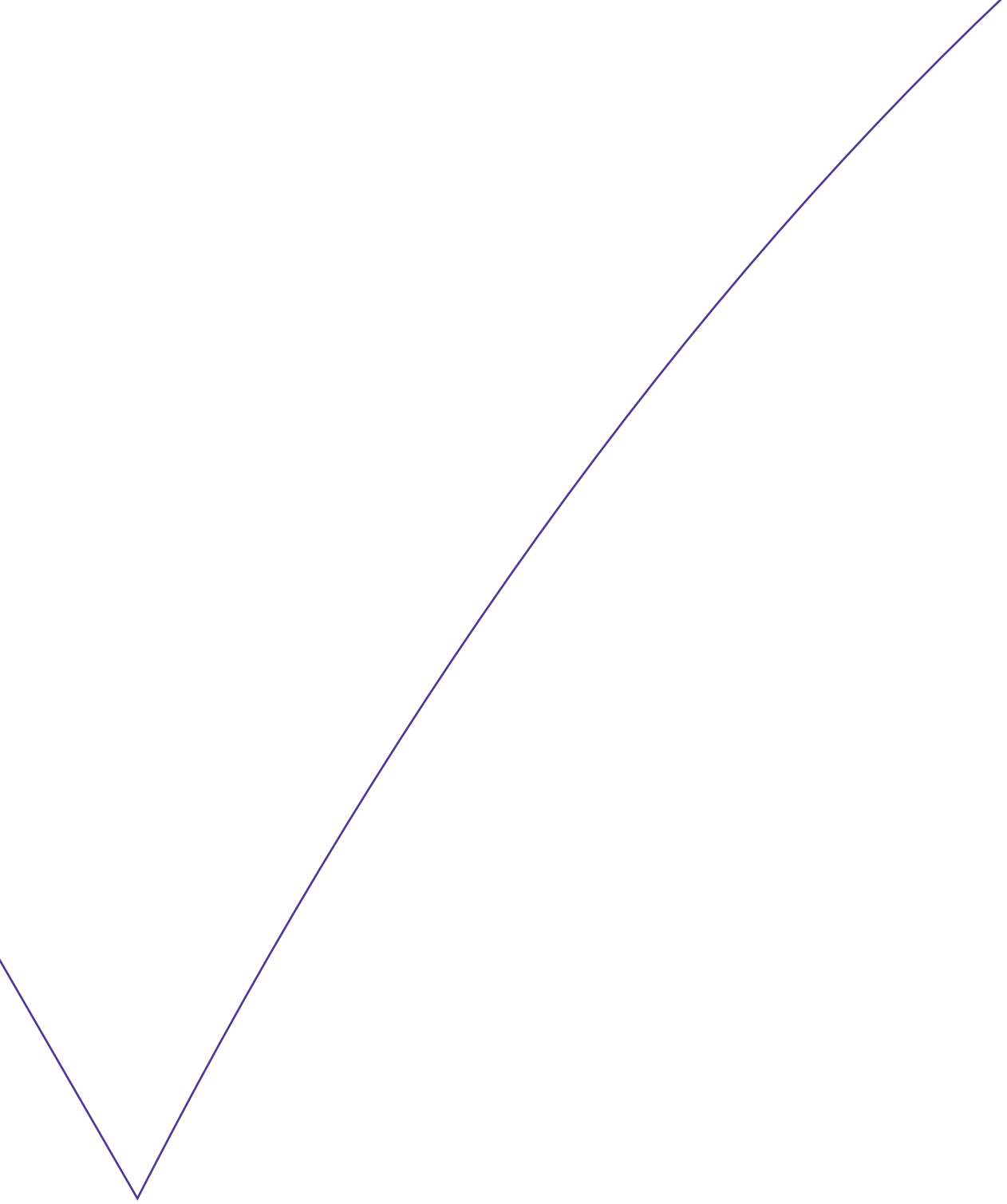
It will be important to have this clarity as soon as possible to allow for enough time to implement required changes. Organisations should prioritise practical steps to mitigate the impacts of GDPR regarding their existing outsourcing arrangements.

In the short term this will likely mean:

- Organisations (both buy and sell side) will need to review and assess current outsourcing arrangements to determine the current 'risk-gap', identify what needs to change and establish a programme to agree the required contract changes, process changes, or even technological changes to be made.
- More focus on detailing the technical and functional data scope of third party infrastructure providers' solutions. Detailed data use case flows will need to be understood, modelled and documented.
- There will be no "grandfathering" of pre-existing contracts
- Outsource contracts expiring after the GDPR takes effect, change control or change of law clauses will need to be included now
- Reviewing the need for standardised solutions to fit an organisation's legacy data environment; in particular those legacy systems where data flows through an organisation may be poorly documented; and the data 'touch points' unknown.

Going forwards, all future outsource arrangements will need to take great care and attention to the GDPR principles.

In this Insight, Wavestone has provided an overview of the changes, and impact the GDPR Directive presents to outsourcing arrangements. Furthermore, it provides a high-level view of some of the key steps companies and service providers should be taking to address and mitigate the impact prior to the effective date in May 2018.



WAVESTONE

www.wavestone.com

Wavestone is a consulting firm, created from the merger,
of Solucom and Kurt Salmon's European Business (excluding retails and consumer goods outside of France).

The firm is counted amongst the lead players in European independent consulting.

Wavestone's mission is to enlighten and guide their clients in their most critical decisions,
drawing on functional, sectoral and technological expertise.