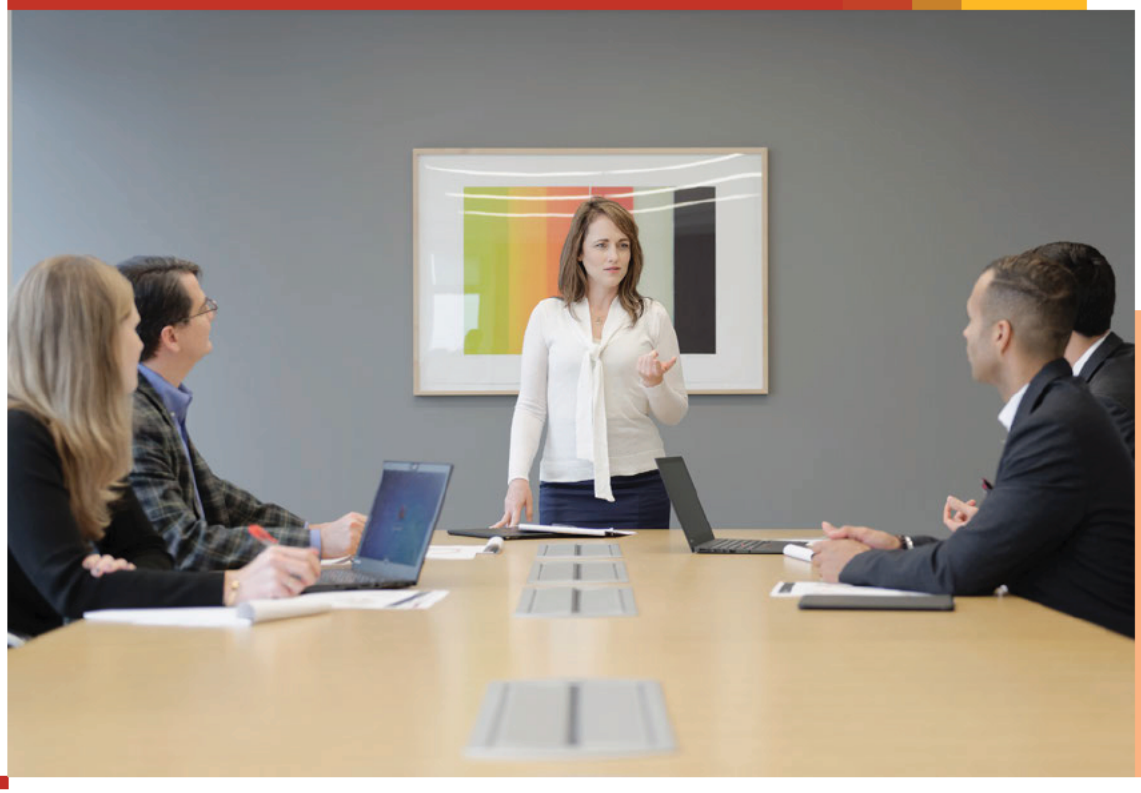
www.pwc.co.uk

General Data Protection Regulation (GDPR)

Bulk data processor contract analysis and remediation service

March 2018



pwc

The GDPR has introduced a variety of new compliance requirements for organisations that process personal data. Amongst these changes are new, more expansive rules on the content of written contracts between controllers and processors. The GDPR further stipulates certain specific terms which at a minimum must be included in those contracts.

For controllers, understanding your third party relationships and ensuring that you have contracts in place that are fully reflective of the requirements of the GDPR, specifically the requirements set out in Article 28, is therefore a must.

For processors, taking a proactive approach to addressing this issue, for instance by defining standard clauses and communicating these to your clients, could make the difference between being in control and being overwhelmed with a variety of proposed wording. Being on the front foot may provide strong competitive advantage.

PwC's GDPR bulk data processor contract analysis and remediation service uses tried and tested methods that combine technology, human resources and subject matter expertise to deliver cost and time effective support and usable outputs for what might otherwise be a daunting exercise if tackled wholly in–house.

Whilst we have focused here on the issue of remediation of data processor contracts within the meaning of GDPR Article 28 our solution can also be applied to the other types of contracts which apply in the context of data protection:

- Those that cover the relationship between the data controller and the data subject e.g. customers or employees
- Those which address international data transfers e.g. model clauses
- Those covering data sharing schemes between different legal entities, e.g. within industry groups or between public authorities

What's on your mind?

Are we a data controller or processor?

Our organisation fulfils many roles when it comes to GDPR – in some situations we are a joint, and in some the sole data controller, in others we are data processors and at times we act as a sub-contractor to other data processors. How do we ensure we address adequately the commercial confusion arising not to mention the associated obligations and liabilities?

Who should be driving action in relation to Article 28 – is it data controllers or data processors?

We have many commercial relationships that are impacted by Article 28 of the GDPR. Where we operate as a controller, should we be educating our processors on their contractual obligations or will that mean we are assuming responsibility for their compliance? Where we are operating as a data processor, should we pro actively engage with our business clients to help them get ready?

How do we know that we have identified all GDPR impacted third party suppliers?

We have relationships with a significant number of third party suppliers but we do not know which are impacted by the GDPR i.e. which are processing personal data on our behalf. What should we do if we haven't got complete records of our contractual relationships? Do we even know where all of our contracts are and who owns them?

How can we prioritise our contracts so that we update the most important ones first?

With so many contracts to review how can we identify the highest risk/priority contracts to ensure they are tackled first? What would constitute a high risk or priority contract? Are some contractual arrangements more – or less – risky than others?

How do we know we have identified all contractual clauses that need updating or adding in light of the GDPR?

We have many contractual documents. How do we ensure that we don't miss a key clause that should be amended? How do we ensure we deliver on all of the GDPR requirements? And, how will we know that the provisions we make are adequate?

Whether we are controller or processor, how do we build an appropriate paper shield and evidence that we understand our accountability obligations in relation to GDPR Article 28 in particular?

How can we best track and record the steps we have taken to review and update our contracts so that we generate the necessary artefacts within the appropriate timelines to evidence our decisions and outcomes? What does good look like in this regard? What position are the regulators taking? Do different contracts have different rules?

End-to-end, this whole process sounds incredibly time consuming. Are there any steps we can take to expedite the activity?

We are already extremely stretched, particularly those with specialist skills needed to support this activity. How can we use scarce resources most effectively? Are there any tried and tested approaches that we can adopt which will save time?

What happens if all of our contracts are not updated and in place by 25 May 2018?

Our business expects to be compliant by May 2018 although we haven't specifically discussed what it means to be in a state of non-compliance. Would we have a defensible position if all of our contracts were not updated in line with the requirements of the GDPR? Should we prioritise fixing our data processor contracts over other GDPR issues?

How can we ensure that we maintain an appropriate level of engagement with and awareness of our data processor's activities?

We know that complying with GDPR Article 28 is not just about pre contractual due diligence, but we are unsure what steps we should take to ensure contractual provisions are adhered to once agreed. For example: how frequently should our data processors be updating us on their activity and what information should we expect them to provide? Can we rely on our data processor's own updates and reports without visiting their premises or without an independent audit? How frequently and what type of additional checks should we carry out?

What about other contractual documentation impacted by the GDPR?

We know that other types of contracts will need to be reviewed and potentially updated in light of GDPR e.g. our employment contracts. How can we make sure we have identified all other relevant contract types and that they have been updated appropriately and are enforceable?

Our point of view

Trusted relationships are key

Organisations acting as data controllers should not underestimate the level of dependency which they place on – and the expectations they have of – third party data processors. It's worth remembering that GDPR requires that *'... data controllers must only appoint data processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected'.*

Adopting a collaborative approach in undertaking your contract reviews will pay dividends.

Controllers you should communicate with your processors about your plans for contracting. Keep them updated throughout, particularly to advise of any actions they may need to take, including reviewing updated documents, attending discussion meetings etc. and then keep that positive engagement in place going forward.

And data processors, you should not underestimate the benefits of developing a trusted working relationship with your clients.

It's not all about the words, due diligence extends post contract updating

From both the data controller and data processor perspective, updating your contracts is key but so is ensuring that the process is not simply about words on paper but about the actual delivery and activity that happens in practice.

Effective contracts can be used as a tool to test and assure delivery. For all parties, it's essential not only that appropriate details are included to address compliance, quality control and assurance issues but further that these provisions are kept under constant review for appropriateness, content and frequency.

Third party contracting risk is a known risk

The Data Protection regulatory environment has looked at the importance of controller-processor contracting in a number of landmark cases. Contractual failures are well understood as being a real contributor to operational failures, such as security breaches, over-retention and over-use. Failing to address GDPR contractual agreements creates a risk that can lead directly to enforcement action in serious cases.

Controllers, don't wait for your suppliers to act

The GDPR and the ICO's guidance makes it very clear that *'Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected'.*

A complacent approach that assumes your third parties will sort out any updates to your contracts will leave you on the back foot and potentially at risk of no action being taken at all.

Suppliers, you can strengthen your commercial position by helping your business clients to handle Article 28

If you are a data processor you may stand out from the competition by showing a proactive approach to contract renewal. Mapping out how you will deliver strong controls for personal data, how you will cooperate with and support your controller and how you will manage the handling of security breaches and incidents, will enable you to engage constructively with your business partners.

Don't put the data you are controlling at risk

Controllers must ensure they have a complete and accurate understanding of the role and performance of their processors. Could you, with confidence answer these questions: Do you know whether any of your suppliers are sub-contracting elements of their processing? Do you know where the processing is taking place? Do you know what training they provide to their employees? Do you know what security procedures they have in place?

Working smart saves time

There are steps that can be taken to help minimise the amount of time this exercise takes and the level of input needed from scarce, specialist resources. Many of those we would recommend are in the human elements: for example, effective and clear internal and external communications is one key area where additional care, attention and planning can deliver significant value. Additionally appointing a Project Manager to oversee the exercise might appear at first glance to be overkill but experience proves that this is one of the most worthwhile appointments that can be made.

What good looks like

Discovery/ Preparation	You have defined clear roles and responsibilities for undertaking contractual reviews, including the appointment of a Project Manager
	You have established a process for documenting, tracking progress and reporting the planned end to end process for GDPR contract remediation
	You have identified all of the relevant i.e. GDPR impacted, third party relationships across your entire enterprise (and created a list of those that are out of scope)
	You have identified the business owner for each relationship (and where none exists)
	You have identified the appropriate contact for your organisation at each third party (and where there is no identified contact)
	You have communicated with your third parties about your intention to undertake a contractual review in light of GDPR and you have outlined the timeframes you are working to and the expectations you have of them in the process
	You have physically located all of the most up to date contractual documents applicable to these relationships
	You have defined escalation routes for issues arising, such as failure to locate contractual documents relating to an ongoing supplier relationship or where no business owner has been identified for that supplier
Drafting	You have drafted new GDPR compliant data privacy contract clauses and obligations to be used in all third party personal data processing contracts going forward
	You have agreed your negotiation parameters, such as liability thresholds, where applicable
Analysis	You have conducted an exercise which digitises your existing contractual documents and then uses an automated process to locate relevant clauses and compare them against your new GDPR compliant clauses if these have already been defined. The outputs of this exercise are provided in a usable format and a full audit trail is maintained
	You have identified which contracts can be updated by notification and which need engagement/discussion with the other parties
Updating	You have addressed any gaps in internal roles and responsibilities for data processor relationships
	You have prepared updated versions of all impacted contracts
	You have checked the provisions in these contracts against GDPR Article 28 and prevailing regulatory guidance
	You have notified and/or agreed the revised terms with the other party and have auditable evidence of these exchanges
	You have agreed what detail, in what format and on what frequency your processors will provide contract performance assurance information to you. This will reflect the nuance of each service contract
BAU	You have implemented a robust process, including defined roles and responsibilities for managing existing and new contracts in compliance with GDPR as part of BAU
	You have created a robust and reliable database containing all existing and new GDPR impacted contracts for which clear management and maintenance accountability has been defined and agreed
	You have defined a clear process for reviewing and where necessary responding to the assurance information being provided by your data processors to ensure issue raised are addressed and that the information provided remains fit for purpose
	You have defined a process for engaging your audit and other relevant teams in due diligence throughout the life cycle of all data processor contracts

How we can help?

Discovery
Find and identify contracts for review
1

Drafting
Draft template GDPR clauses
2

Analysis
Analyse contracts
3

Update
Update and implement contracts
4

BAU
Establish process for managing new and existing contracts
5

Our GDPR bulk contract analysis service has been designed to provide support for the end to end lifecycle of GDPR contractual analysis and remediation, from the initial preparatory/discovery phase through drafting your GDPR compliant clauses, analysis of your existing contracts, updating your contracts and implementing a robust BAU management process.

Whatever stage you are at and whether you need to access the entire end to end service or selected elements we can provide relevant, experienced support – mobilised at speed.

When to act

The Regulation was conceived in 2012 and the full text announced in April 2016, and as such, it would be indefensible to suggest that progress has not been made due to a lack of awareness. Alongside the text of the GDPR the European Data Protection Authorities (including the ICO) frequently publish blogs and guidance on the GDPR and although there are still a number of areas that remain unclear, there is enough guidance for businesses to have used the two year grace period to have begun making the changes required.

The sooner you can begin what may be a very time consuming exercise the better.

What needs to be included in the contract?

Contracts must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller.

Contracts must also include as a minimum the following terms, requiring the processor to:

- *only act on the written instructions of the controller;*
- *ensure that people processing the data are subject to a duty of confidence;*
- *take appropriate measures to ensure the security of processing;*
- *only engage sub-processors with the prior consent of the controller and under a written contract;*
- *assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;*
- *assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;*
- *delete or return all personal data to the controller as requested at the end of the contract; and*
- *submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.*

Source: ICO Guide to the General Data Protection Regulation (GDPR)

What you gain

- ✓ ***A proven methodology*** – we have worked with a number of global clients in order to help them review and remediate high volumes of contracts in light of regulatory changes. Our data processor bulk contract analysis and remediation service utilises our existing technology and human resource frameworks, our extensive experience in performing bulk contract analysis in combination with our GDPR expertise.
- ✓ ***Risk and cost reduction*** – our approach – whether you opt for support in a single, focussed area or the end to end process – delivers both risk and cost benefit. We will help you take an informed risk based approach which will instil confidence in all parties. Our use of human and technical resources delivers effective costs savings and enables decisions and progress to be made at pace.
- ✓ ***A personalised service*** – we can support you through the entire end to end lifecycle or any phase or sub phase of activity on your contract review activity. We include extra time at the beginning of each analysis phase to fine tune the software to your organisation's contractual 'nuances'.
- ✓ ***Best use of technology*** – our solution uses proven technology fine tuned to the language of Data Protection clauses in varied contracts to conduct the document digitisation, analysis and reporting.
- ✓ ***Usable outputs*** – in contrast to spreadsheets, which are often used as the output format for exercises of this nature, our chosen technology provides a suite of usable, informative interactive dashboards. They enable you to drill down into the detail of your contracts to understand immediately any issues or opportunities arising. These reports establish the baseline on which you can generate the necessary artefacts within the appropriate timelines to evidence your decisions and outcomes.
- ✓ ***Consistency*** – using specialist software trained to locate 'Data Protection' elements ensures a level of consistency that cannot be provided through a wholly manual approach.
- ✓ ***Speed*** – our system and people are ready and trained. We can mobilise a team at speed and the approach we have designed provides a far higher throughput rate than a manual process.
- ✓ ***Quality control*** – notwithstanding the use of technology, we recognise that the human element is also essential in processes such as this. Our experienced Quality Control specialists will ensure that gaps and inexplicable inconsistencies in the analysis/outputs produced are minimised.
- ✓ ***A scalable team*** – the volume of contractual documents to be reviewed and remediated can vary hugely from organisation to organisation. That's why we have defined an approach which provides complete flexibility: the size of the team that will support your contractual review will be determined by the volume of documents to be analysed and the time frames within which you wish to undertake the exercise.
- ✓ ***A multidisciplinary approach*** – PwC contract analysis team will comprise of data protection experts, legally trained analysts, risk and control advisors and programme management consultants. All with deep subject matter expertise.

Contacts

Stewart Room
GDPR Strategy, Law and Compliance
Partner, PwC UK
E: stewart.room@pwc.com

Fedelma Good
GDPR Strategy, Law and Compliance
Director, PwC UK
E: fedelma.good@pwc.com

Craig McKeown
GDPR Computer Forensics and Data Analytics
Director, PwC UK
E: craig.l.mckeown@pwc.com

Mark Hendry
GDPR Strategy, Law and Compliance
Senior Manager, PwC UK
E: mark.hendry@pwc.com

www.pwc.co.uk

180312-172209-MR-OS