



GDPR AND OUTSOURCING - BUSTING THE MYTHS

CONTENTS	2
1. GDPR - BUSTING THE MYTHS	3
2. WHAT IS GDPR TRYING TO ACHIEVE?	3
3. DOES THE NEW GDPR MEAN I SHOULD STOP OUTSOURCING?	4
4. HOW DOES THE GDPR AFFECT MY OUTSOURCING CONTRACT?	5
5. HOW DOES THE GDPR AFFECT MY OUTSOURCING CONTRACT? PT. 2	6
6. WHAT DO I NEED TO CONSIDER WHEN IT COMES TO CONTRACT RENEWALS?	7
7. WHAT DO I NEED TO DO TO BE GDPR READY?	7
8. WHAT IS DDC DOING TO SUPPORT OUR PARTNERS?	8

Thanks to the following contributors:

Mike Donoghue, Managing Director, *Economit*

Sara Ludlam, Partner, *3volution*

Michelle Davies, Programme Director, *DDC Outsourcing Solutions UK*

1. GDPR – BUSTING THE MYTHS

Unless you've been on an extended holiday on a Caribbean island for the last two years, you will have no doubt been made aware that the new GDPR comes into force on 25th May. Everyone has an opinion on the matter, and many comments have been made about the huge fines that will be imposed upon the companies that are found to be non-compliant. We've decided to pull together some pertinent information that will hopefully help to put you at ease regarding outsourcing your processing activities, and bust many of the myths surrounding this latest piece of business-critical legislation.

2. WHAT IS GDPR TRYING TO ACHIEVE?

In a blog piece from August 2017, Elizabeth Denham, Information Commissioner, set about explaining the reasoning behind GDPR. She started out by stating that GDPR was not about making money from large fines.

The GDPR endeavours to put the data subject back in control when it comes to their personal information, and aims to ensure that businesses give their clients, their client's customers, and their client's end-users confidence in the services that they provide.

The GDPR replaces the Data Protection Act from 1998, and modernises the laws governing how personal data is processed. This modernisation takes into account the digital world we are all now a part of, and requires organisations to better understand the data they are processing. This includes knowledge of where the data is stored, and whether they have reasonably considered the risks involved in all processing activities. The good news is that if you are compliant with the current Data Protection Act, then there should not be a lot of work to make you compliant with the new regulations that come into force on 25th May.

The GDPR endeavours to put the data subject back in control when it comes to their personal information, and aims to ensure that businesses give their clients, their client's customers, and their client's end-users confidence in the services that they provide.

3. DOES THE NEW GDPR MEAN I SHOULD STOP OUTSOURCING?

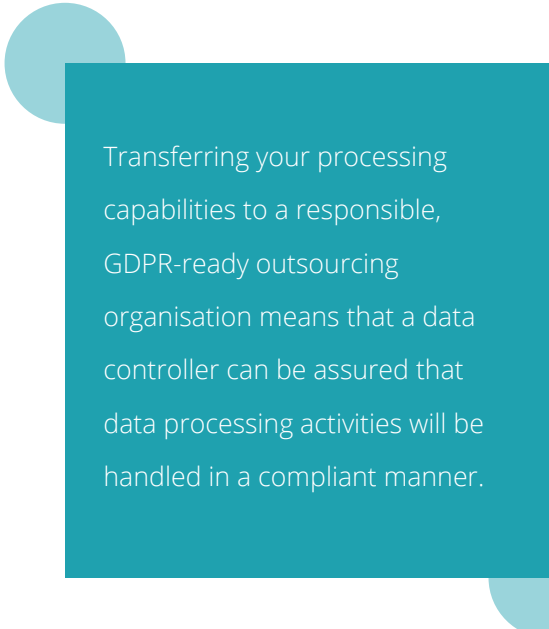
In short, no; and there are a variety of reasons why not. The new GDPR ensures that both you and your outsourcer be transparent about the systems and processes used for processing data. To that end, you are actually getting an extra level of security from your outsourcer, with an extra pair of eyes ensuring everything is within regulation.

Your relationship with good outsourcers will not be affected as they will already have in place the required data protection systems, and will be looking to show you how they comply and how they can help you to comply.

It is also worth noting that although the GDPR will become law, not all organisations will be fully compliant when it comes into force in May 2018.

Transferring your processing capabilities to a responsible, GDPR-ready outsourcing organisation means that a data controller can be assured that data processing activities will be handled in a compliant manner.

As a result, there are benefits to outsourcing in regards to GDPR, including the fact that data processors (your outsourcers) acquire legal responsibilities in relation to processing personal data, so they are now legally motivated to help you get it right and will be improving the security of your customers' personal data.



Transferring your processing capabilities to a responsible, GDPR-ready outsourcing organisation means that a data controller can be assured that data processing activities will be handled in a compliant manner.

4. HOW DOES GDPR AFFECT MY OUTSOURCING CONTRACT?

The legal changes, in brief, are as follows;

CHANGE 1:

You must have a written agreement in place with all of your “data processors.” In this written agreement, you will need to;

1. Identify what personal data is to be processed by your out sourcer
2. Identify what “processes” are to be carried out on that personal data
3. Identify what the appropriate security and organisational measures are, which need to be implemented, bearing in mind the level of risk associated with a GDPR breach for the type of data being processed. There may be different measures for different types.

A good outsourcer will be able to work with you to advise, manage, and where necessary adapt your data processing systems, establishing what the appropriate security and organisational measures should be. Those with experience and a proper understanding of GDPR should make it easier for you to comply with the additional obligations and ensure that you minimise the risk relating to the processing of personal data.

A good outsourcer will be able to work with you to advise, manage, and where necessary adapt your data processing systems, establishing what the appropriate security and organisational measures should be. Those with experience and a proper understanding of GDPR should make it easier for you to comply with the additional obligations and ensure that you minimise the risk relating to the processing of personal data.

CHANGE 2:

Any written agreement should include the following rights for you;

1. To audit your data processor and any sub-processors to check they have the appropriate security and organisational measures in place. Again, an effective outsourcer will have efficient, effective GDPR-compliant systems in place, making this obligation easier and cheaper for you to effect.

It should also have the following obligations for the outsourcer/data processor;

1. To comply with the GDPR and in particular
 - a. To respond quickly to any data subject access requests (you will have 30 days instead of 45 days to respond to the data subject)
 - b. To report promptly and in any event within 24 hours of any breach (you will have 72 hours to consider whether a breach needs to be notified to the relevant Supervising Authority (which is the Information Commissioner's Office in the UK))

You will know you are working with the right outsourcer when they volunteer the agreements they have in place with their non-EEA based sub-processors and that these comply with the GDPR.

A good outsourcer will have systems in place that are designed to facilitate not just the quick and efficient recovery of specific personal data, but also the ability to amend, rectify, transfer, and delete personal data, as well as allowing the processing of personal data for certain specified purposes but not for others.

An outsourcer who is proactive about the security of personal data will not just reduce your risk of a breach but will also suggest improvements in your own systems to improve security and compliance with GDPR.

Don't forget that when your outsourcer is transferring personal data outside of the EEA, to a country that has not been assessed as "safe" by the EU Commission, or if it is to a company in the US which is not certified under the "Privacy Shield" programme, then you will need to get confirmation that your outsourcer has the correct agreement in place with the entity outside the EEA that is receiving the personal data.

You will know you are working with the right outsourcer when they volunteer the agreements they have in place with their non-EEA based sub-processors and that these comply with the GDPR.

5. WHAT DO I NEED TO CONSIDER WHEN IT COMES TO CONTRACT RENEWALS?

Inevitably, you will be in the middle of agreements with outsourcers on 25 May 2018. It is important that such agreements are reviewed and, if necessary, updated before this date to comply with the GDPR. DDC Outsourcing Solutions UK's (DDC's) team of experts can help you identify what, if any, changes are needed. They can also help you to review your agreements and advise you on the best course of action for your business.

6. WHAT DO I NEED TO DO TO BE GDPR-READY?



Check your agreements with your data processors, updating them if they do not comply with the GDPR. DDC have compliant updates ready to go, or if you prefer we can work with you to vary existing terms or agree on new terms to comply.



Check the personal data that you process and that you want third parties to process on your behalf. Record the legal basis on which you are relying for such processing and if this is consent, check that you have recorded those consents and that they are up to date.



Ensure that all processing activities have been risk-assessed from both the controller and the processor's perspectives. Both parties should have an active role in risk management under the GDPR, which demands particular focus in this area.

7. WHAT IS DDC DOING TO SUPPORT OUR PARTNERS?

DDC have already been working with our existing partners for some time to ensure that our joint obligations under the new incoming laws are met, and that both parties have the lawful processing of personal data and security at the fore of everything we do together. Just some of the actions we are taking:

- We will work together with our partners to ensure procedures are put in place, so that subject requests of all types can be dealt with in the most efficient manner.
- We will ensure the security of the data we process, by further strengthening our technical and organisational measures of protection, and ensure it is kept confidential.
- We will ensure that all of our contracts are GDPR relevant, and specifically designed to protect our client's interests as well as our own. We will manage risk on behalf of our clients at all points for each respective processing journey placed under our responsibility.
- DDC's ethos is to always employ a consultative approach when dealing with our partners - and this value-added service is typically instrumental in helping us achieve not only compliance with the regulation, but also an efficient, accurate, and secure processing solution.

Since the GDPR was announced several years ago, DDC has made considerable investments in people and technology to ensure that our clients and their processing activities are compliant and ready for May 2018.

For more information on how the new GDPR regulations will affect outsourcing for your business, contact DDC today.

DDC



Outsourcing Solutions UK

☎ 01909 488600

✉ enquiries@ddcos.com

🌐 ddcos.com

RISKVIEW

Effectively manage GDPR risk and adhere to the regulation quickly and easily – without having to become a compliance expert.

RiskView gathers data from individual computers, analyses its risk profile and grades it according to the amount of non-compliant data held.

Our assessments provide an audit trail that demonstrate care and progress in regulatory areas. Allowing your organisation to report risk with confidence and provide evidence to satisfy GDPR review – quickly and efficiently.



RiskView allows you to focus on your core business, while identifying and delivering fast and easy compliance assessments to prepare you for the GDPR. Contact us today and find out how to begin your journey to compliance.



Locate unprotected Personal Identifiable Data (PID).



Focus your resources only on what is needed to become compliant.



Identify security threats in everyday system usage.



A key component in achieving and maintaining GDPR Compliance.



Improve user accountability and compliance with internal rules.



Rich visual set of analysis tools helping you to effectively manage your GDPR risk.



A detailed view of your company's data storage.



Identify sources of critical data leakage.



@DDC_OS



/company/ddc-os