myerson

Tech Lite

Spring 2019

Articles in this issue:

www.myerson.co.uk
0161 941 4000

Welcome to Myerson Tech Lite

At Myerson Solicitors we have the experience and expertise to provide advice to those working within the IT, IP and Data Protection industries and in this issue our experts look at:

Tech Lite

Predictions then and now - where are we in 2019?

At the start of each year it has become a tradition for us to make a number of predictions for the year ahead and to reflect on the results of our crystal ball gazing from the year before. Now the results are in, how did we do?
Last year we made the following predictions:

- Emergence of Blockchain platforms offerings as an alternative to traditional cloud platforms. While Blockchain has not swept all before it over the past year, we have seen a small number of platforms and applications starting to use Blockchain technology. Could this be the start of the much hyped technology bearing fruit?

- Software developers to come under greater scrutiny from customers looking for software security guarantees and reassurances. Tied in with GDPR, customers now have greater responsibility to ensure that software and other IT systems are secure. We have seen this manifesting itself in greater customer due diligence being carried out on the security of supplier systems and in the form of greater contractual obligations and remedies being imposed.

- Artificial intelligence and machine learning to become mainstream and the norm in business operations. What next, conversations with bot call handlers? In some industries, this has already arrived! We have certainly seen artificial intelligence being used more and more in ever more ingenious ways. As well as chatbots becoming more prevalent, there are more firms offering bespoke development of AI based solutions for use in businesses, particularly in the area of data collection and analysis.

We anticipate AI will continue to grow and be put to increasingly diverse uses.

So what about the coming 12 months? Our predictions for 2019 are as follows:

- Brexit – we boldly predict that Brexit will or will not happen in 2019 and that its effects will be far ranging or, alternatively, there will be no effect whatsoever. Or maybe somewhere in the middle. There are a number of governmental plans in place for the various scenarios, which we have reported on previously, and we will be continuing to monitor the legal developments as political events continue to play out in Brussels and Westminster.

- Data protection fines – now that GDPR is in force we expect regulators to impose some heavier data protection fines over the next 12 months, continuing the trend we reported in **our article earlier this year**. However, we do not expect to see a fine at the full level of the 4% turnover of a global business for some time – given the enormity of a fine at this level a particularly flagrant data protection breach would be needed, as well as regulators choosing to take a very hard line approach. While possible, we do not expect to see fines at this level for a number of years.

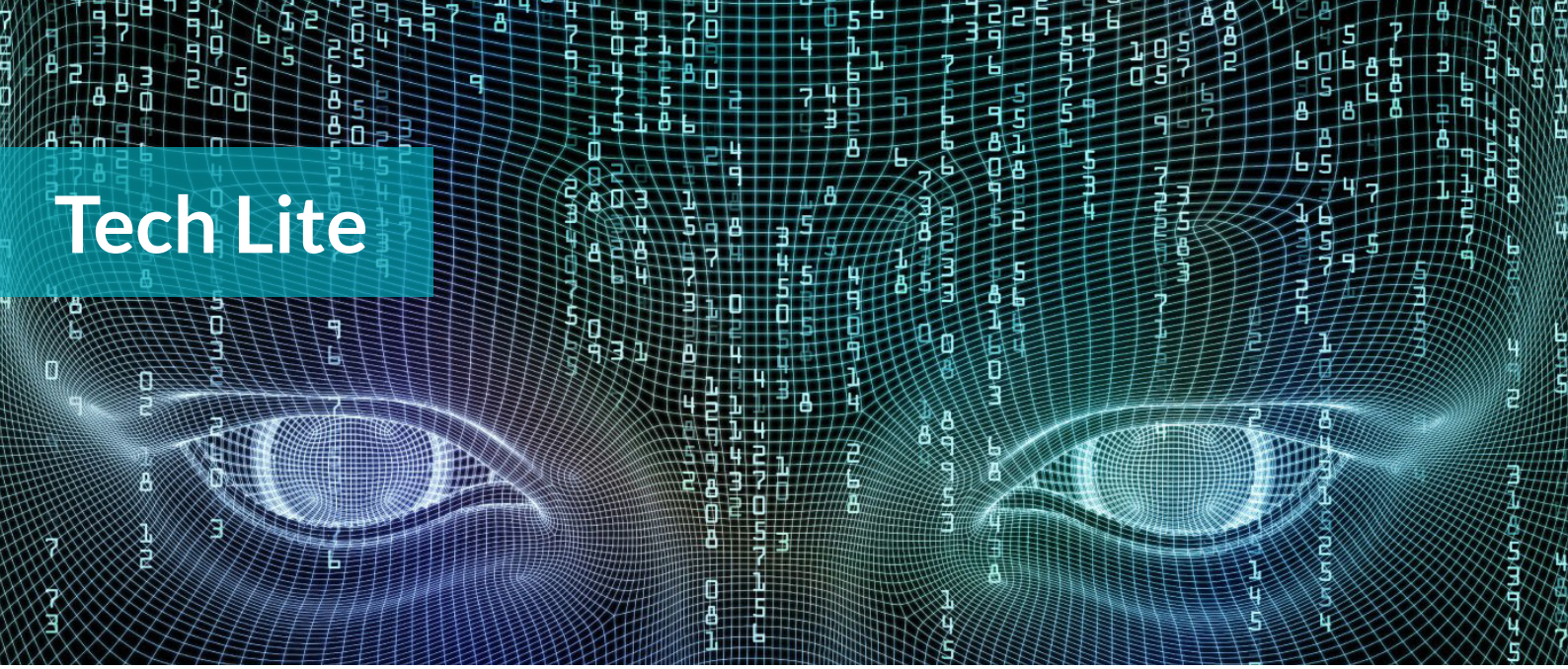
Tech Lite

- Regulation of social media – we predict that there will be further controversies coming to light, hot on the heels of the **Cambridge Analytica scandal,** particularly in the realms of dissemination of disinformation and the use (or misuse!) of personal data. We anticipate that regulators and governments will be looking to impose stricter rules on social media platforms and subject them to greater scrutiny

- Quantum computing – we predict that there will be increasing hype around quantum computing, due to the exciting prospect of its mind-bending possibilities. However, we predict that it will be a number of years before any commercially viable product is on offer (if it ever is!).

Of course, only time will tell whether our predictions will come true and we will check back in again this time next year to report on whether Mystic Meg needs to look anxiously over her shoulder…

If you would like to discuss any of the issues raised in this article or require advice in relation to technology matters, please contact our experienced **IT & Technology Team**.



Tech Lite

Is Artificial Intelligence closing the loop on recruitment?

"Closing the loop" is a concept that has been widely adopted in the manufacturing industry and process for years; identifying problems early on in the chain to prevent poor quality products as the output. Automation allows this concept to be performed with minimal human interaction. Add to this the advent of artificial intelligence and the application of this concept is far reaching. One area AI is being used to "close the loop" is the recruitment process potentially revolutionalising how businesses make the decision on who to employ. It's recruitment Jim but not as we know it.

According to the Deloitte Human Capital Trends report published last year, 38 percent of companies use AI in their recruitment process, and this figure is expected to increase to 62 percent during the early part of this year.

The potential benefits of minimal human intervention and assessment against known measurable determiners can be an attractive notice. This is particular so as recruitment has historically relied purely on human judgment and inevitably therefore carries the risk of human error. Whilst it is still important to encourage the "personal touch", the introduction of predictive data analytics and other AI tools lower the threshold for businesses making expensive mistakes in their recruitment processes.

Automation has and can enhance the recruitment process in:

Candidate screening - software solutions can be used to screen for the right people by looking beyond their CV for example scrapping data from their "digital online footprint" and analysing their online presence to assess their suitability.

The interview process – interviews by automated videos. It allows pre-set questions to be viewed and answered by candidates at a time and place that suits them, and can be reviewed and analysed at a time to suit the business, saving time and resources. Responses can also be analysed and compared.

Feedback on this form of interviewing has been overwhelmingly positive as video interviewing can promote a feeling amongst candidates that they are being treated as fairly as everyone else, therefore it looks set to become a fast growing trend in 2019.

Psychometric tests - Harnessing the power of big data analytics such technologies put candidates through a series of tests to determine their skills, critical thinking and creativity, by using thousands of different data points. This can be invaluable in enabling businesses to make the correct decisions about whether a candidate has the requisite skills to succeed in the role. It can also be used by business to determine which employees are suitable for promotions.

Potential Pitfalls

As the AI in this field becomes more sophisticated, software solutions are enabling business to automatically analyse an ever increasing array of data sets, scrutinising everything from values, goals, aspirations, even the language used in LinkedIn posts.

Tech Lite

With these types of practices, it is of course important to ensure that your business is mindful of data protection laws, including GDPR, to ensure that you are compliant and are not unlawfully processing data and minimise your risk exposure.

What can we do?

Although tech may "close the loop" on some aspects of the recruitment process, businesses must be careful not to replace the human touch altogether. Like humans, even robots can make mistakes, as Amazon found out last year. Its AI recruitment system that it had been developing, taught itself to discriminate against women, actively downgrade CVs which had any references to "women" or "women's". The system was trained using 10 years worth of CVs, however, most were from men so the AI had learnt to give more prominence to male CVs. Reports suggest that the system hadn't been used live but it does go to the route of AI in that it's only as good as that data input and what it has to learn from.

So, whether you are developing the next big app/automated service or looking to:

a) implement an Automated Recruitment Testing & HR system "Arthur" – Alexa's big brother; or

b) simply undertake some automated profiling, our IT team are on hand to "close the loop" on your legal requirements and can assist and advise your business on the following aspects:

- raising finance to get your product developed;
- taking your product ideas to market and protecting your rights;
- licensing and implementation terms;
- data protection; and
- potential claims or employment proceedings should AI go array.

Our specialist IT & Technology team has over 20 years' experience working in the technology sector including both the regulatory technology sector (RegTech) and financial technology sector (FinTech). We regularly advise businesses in respect of the various legal, contractual and regulatory issues that face both suppliers and customers in this sector.

Please contact our **IT & Technology Team** us if you wish to discuss your use of Artificial Intelligence in your business or your compliance with data protection laws.

Other article reviewed:
https://www.lhh.com/our-knowledge/2018/how-artificial-intelligence-is-changing-the-hiring-process

Tech Lite

Cloud Computing & Data Protection

Cloud computing is now commonplace in the business world and often involves the storing and/or processing of personal data. Therefore data protection must be considered carefully, particularly in light of the General Data Protection Regulation ((EU) 2016/679) **(GDPR)** which came into effect on 25 May 2018. In this article we consider some of the key aspects of the GDPR that cloud service providers and their customers need to be aware to.

Does the GDPR affect me?

In all likelihood, yes. The GDPR applies when either:

a) the customer OR the cloud service provider is based in the EU; and

b) personal data is stored, transferred or otherwise processed.

Cloud service providers based outside of the EU will be caught if their customers are based in the EU. Equally, cloud customers will be caught if they are based outside the EU and their cloud provider is based in the EU and personal data is processed. The GDPR will still need to be considered by UK entities who will trade with EU member states after Brexit.

The territorial scope of the GDPR is particularly important with cloud computing, since it is very common for an EU customer to use a non-EU cloud service provider, or an EU cloud service provider to use data centres which are based outside of the EU. At present, it is unclear whether enforcement action can be taken under the GDPR against a non-EU entity and therefore the impact this may have on a non-EU entity's willingness to work with an EU entity is unknown at this stage.

Controller vs processor

Typically cloud service providers have little or no control over the personal data that they process, how it's collected and the purpose for which it's collected, so are therefore simply "processors". Some cloud service providers have gone as far as to only deal with encrypted data, to minimise their risk exposure under the GDPR.

Cloud customers are generally the ones who have control over the data they upload to the cloud, the purpose for which they are collecting the data and the use to be made of the data and therefore are the "controller" of the data. As controllers, there are additional obligations to comply with under the GDPR, including ensuring that data is not stored for longer than is necessary and is only used for the purpose notified to the individual at the time their data was collected.

However, even where cloud service providers are processors, they still have certain responsibilities under the GDPR. These include keeping records of their data processing activities, keeping data secure, and cooperating with the relevant regulator in the performance of their duties. They are therefore not able to completely detach themselves from the burden of the GDPR.

How to ensure compliance

A well-drafted contract between the customer and the cloud service provider should set out very clearly how the cloud service provider will handle the data. Be aware, if you are a cloud service provider and you use any personal data you are processing for your own independent purposes or have a certain level of control over the data, you may also be a controller (in your own right) or a joint controller (with your customer). In these circumstances, further provisions

will need to be set out to cater for your additional obligations under the GDPR.

The GDPR envisages that there will be a standard form controller-processor contract created by the European Commission at some point in the future, however this has not yet happened.

Therefore, parties should ensure that their contract clearly sets out the following:

- the subject matter of the processing of data;
- the duration of the processing;
- the nature and purpose of the processing;
- the type of personal data that will be processed;
- the categories of data subjects; and
- the rights of the controller to use that data.

What are the obligations on a processor?

A processor must comply with the following:

- only process personal data on the "documented instructions" of the customer, including when dealing with sending data outside of the EEA;
- have confidentiality commitments from its staff;
- have in place adequate security measures to protect the data;
- assist the customer with data subjects' rights requests (note that they do not actually have to deal with such requests, they just have to assist the controller);
- assist the customer in complying with their obligations under the GDPR relating to information sharing, security, data breach notification and data protection impact assessments (for risk management purposes);
- delete or return data to the customer upon request at the end of the contract – including deleting backed up files; and
- allow the customer to carry out audits and inspections of their data.

Audit Issues

Audits can be a major headache for cloud service providers, not least because of the virtual nature of the technology and the fact that they are likely to be servicing multiple customers. There is the risk that an audit by one customer may breach the cloud service provider's confidentiality and security obligations to its other customers. Unfortunately, the GDPR states that processors must allow a controller to audit unless they can argue that the controller is unlikely to learn much by carrying out an inspection.

Some cloud service providers have found creative solutions to solve this audit dilemma, such as employing a third party to carry out the inspection and produce a report which is then given to the customer. Whilst this may be a solution, some customers may not be happy to accept a report from a third party, and it remains to be seen whether regulators will accept this interpretation of the GDPR.

Sub-processors

Another issue is that the cloud service provider may not operate the data centre where the data is stored, therefore creating a sub-processor arrangement. Sub-processing is not permitted under the GDPR unless the controller has given specific consent (for a particular sub-processor to be used) or general consent (to a list of potential sub-processors, for example). General consent allows more flexibility; however, the cloud service provider would need to inform its customer of every change in sub-processor and allow them an opportunity to object, which may be overly restrictive for the cloud service provider. Any processor-sub-processor contract **must** mirror the data protection obligations in the controller-processor relationship to ensure that all parties comply with the GDPR.

Breaches

Under the GDPR, processors are under an obligation to keep the controller notified of any security breaches. Any contractual obligation to report breaches should not be ignored. If a breach is serious in nature and a reportable breach, the controller only has 72 hours from when it became aware of the breach to report the breach to the ICO. Although there is no time limit for requiring a processor to inform the controller of a breach, the GDPR does say that there must not be "undue delay", so best practice is to report as soon as possible. From a customer's perspective, they may want to add further sanctions on the cloud service provider for failing to adhere to this.

Tech Lite

Transferring data

Both controllers and processors must take care if they are transferring data outside of the EEA. This includes processing data on servers that are located outside the EEA. Where data is transferred to a non-EEA country, that country must have been deemed "adequate" by the European Commission before the transfer can take place. If the country is not adequate, then "appropriate alternative safeguards" must be in place. These could take the form of additional safeguarding clauses in the contract.

Standard contractual clauses have been adopted by the European Commission to ensure an adequate level of protection in these types of situations. However, when dealing with non-EU transfers of data where one party is not subject to the GDPR, these standard clauses cannot be amended. If they are amended, the clauses are not automatically considered to provide an adequate level of protection and are therefore not guaranteed to be GDPR compliant, leading to the view that the standard clauses can be inflexible.

The solution therefore can be to "clarify" some of the language within these clauses in order to make the contract more commercially acceptable (whilst being careful not to amend the standard contractual clauses).

An alternative would be to submit proposed sets of contractual clauses to the relevant national supervisory authorities for approval – although they will still need to undergo the European Commission's examination procedure and may be rejected.

It is possible to transfer data outside the EEA with a data subject's explicit consent, however in a cloud computing context, this may be impractical as it would be impossible for a controller to obtain the consent of every data subject.

Conclusion

Whilst the GDPR has affected many businesses in many ways, cloud services are particularly affected. As penalties for breach of the GDPR are significant (up to 4% of annual global turnover), cloud service terms should not be overlooked.

Don't despair though, our expert Technology and GDPR lawyers are on hand to help you through this data minefield.

We are able to assist with drafting cloud service and hosting agreements:

- reviewing and negotiating;
- subscription service agreements;
- privacy notices;
- data processing addendums; and
- data protection policies and protocols.

Tech Lite

Social Media Influencers

Ja Rule - you fool?

Influence controversy?

It's been reported that Kylie Jenner was paid $250,000.00 for a single Instagram post to promoting Ja Rule's thwarted luxury musical festival "fyre fest". What was not clear from the post and other "influencers" advertising the festival was crystal clear that they were being paid for their post "endorsements".

"SPOILER ALERT"

The Festival, was billed as a luxury festival to be held in the Bahamas in 2017. The festival had never been staged before and used various social media influencers to promote it and create a word of mouth buzz resulting in tickets quickly selling out.

The festival was not as billed, with performers dropping out, luxury accommodation replaced with tents and portions of the site were still undergoing construction when festivalgoers arrived. It was ultimately cancelled within 24 hours having descended into chaos. The founder of Fyre was sentenced to 6 years in prison in 2018 for fraud, as well as being the subject of a $100 million class action lawsuit for fraud, breach of contract and misrepresentation after festivalgoers were stranded on the island without water, basic amenities or means of leaving.

Whilst an extreme example, this shows the effect that social media influencers can potentially exert over their followers. It is this reach that the CMA guidance is now attempting to regulate.

The Competition and Markets Authority has recently released guidance for social media influencers confirming what they must do to make clear to their followers if they have been paid, awarded or incentivised to endorse or review something in their posts.

The new guidance followed an investigation by the CMA in 2018 regarding whether consumers are being misled by celebrities who do not make clear that they have been paid, or rewarded, to endorse products or services online. A similar course of action has also been taken in the US by the Federal Trade Commission.

The guidance applies to any bloggers, vloggers, celebrities and social media personalities, along with PR and marketing companies. The CMA want it to be made clear if a payment or an incentive has been promised in a way which is 'transparent, easy to understand, unambiguous, timely and prominent', as well as being 'apparent without the need for people to click for more information'.

The CMA has confirmed that the following practices do not go far enough:

- tagging the brand;
- using hashtags such as #ad, #spon, #collab etc.; and
- disclosing the commercial affiliation on the influencer's profile page.

Tech Lite

The guidance suggests prominently stating the relationship in a post and utilising the 'paid partnership' tool on social media platforms such as Instagram. However, it gives no clear indication of what will satisfy the suggestions within the guidance, only confirmation of what will not, no doubt because this will change as social media continues to evolve.

The Advertising Standards Authority is currently carrying out research into influencer advertising, with the results expected later this year. The CMA will work alongside the ASA to continue to develop the regulation of advertisements on social media platforms. This is therefore likely to be only the beginning of a more thorough regime to regulate influencer advertising online.

Please contact our **IT & Technology Team** if you would like to speak to someone about social media influencers and advertising compliance. Alternatively, you can call us on 0161 941 4000 or email **lawyers@myerson.co.uk**.

Myerson Solicitors LLP
Grosvenor House, 20 Barrington Road, Altrincham WA14 1HB
Tel: 0161 941 4000 | Fax: 0161 941 4411 | DX19865 Altrincham
lawyers@myerson.co.uk | www.myerson.co.uk | @myersonllp