Birketts

WELCOME TO THE OCTOBER 2018 EDITION OF

Upload

IN THIS ISSUE

Welcome to the latest edition of Upload, bringing you our latest news and insights into the many developments taking hold in technology.

Adrian Seagers
Partner
01223 326613
adrian-seagers@birketts.co.uk

It is difficult to believe the sheer number and scale of issues that technology has brought into the public gaze this year. The Google+ and Cambridge Analytica stories, the advance of AI in the world of work and the threat to the nation's security from cyber-attacks by hostile third parties – all have featured large in the national consciousness.

Technological innovation is the common thread, and the pace is not going to let up. Our own technology practice has seen a significant increase in clients needing advice and support, as they seek more actively (or urgently?) to participate in the opportunities available, or as their own businesses adapt to a changing climate where the impact on society and the individual grow in importance.

In this edition, amongst other matters, Maria Peyman looks at a number of issues regarding cyber security, just ahead of the CBI cyber security conference which we are pleased to co-sponsor this month. Georgina Perrott comments on the regulation of cryptocurrencies and Nicola Gulrajani brings us up to speed on the ICO's grants programme offering funding to companies developing data protection solutions, and Clare Hedges, Head of Immigration, provides an update on employing EU nationals.

There should be something here for everyone.

IN THIS ISSUE

@birkettsllp BirkettsLLP @birkettsllp

Confidential information and how to protect it

Paul Palik
Senior Associate
01603 756496
paul-palik@birketts.co.uk

For many businesses, the protection of information which provides a competitive edge is imperative to success. Confidential information may be disclosed in the course of business for a variety of different purposes such as negotiations regarding a potential business acquisition or commercial exploitation with a third party.

Parties who envisage disclosing confidential information to third parties should ideally enter into a non-disclosure agreement (NDA) in order to provide clarity on the treatment of information provided. Here are some key considerations when entering into an NDA.

1. **Definition of confidential information:** this underpins the information being provided under the NDA. The definition is typically drafted widely, it should cover written as well as oral information. Beware of NDA's that require the disclosing party to subsequently identify in writing any confidential information disclosed orally. The reality is that this is seldom (if ever) done, which potentially leaves orally disclosed information outside the parameters of the NDA.

2. **Exclusions:** an NDA will define what information is not subject to confidentiality. This typically includes information already known, information already in the public domain, information independently produced by the receiving party and information received from a person/entity who owes no obligation of confidence to the disclosing party.

3. **Treatment of confidential information/permitted use:** NDAs should specify how confidential information is to be used and treated. This includes defining a purpose for its use and preventing disclosure outside of that purpose. The NDA should be clear regarding to whom the receiving party may disclose confidential information received (typically employees and professional advisors), and care must be taken to ensure that the receiving party procures compliance with the NDA by those persons. Care should also be taken to ensure that a receiving party treats the confidential information received with a minimum 'reasonable' standard of care. NDAs can often prescribe a standard of care which is measured only in comparison to how the receiving party treats its own confidential information. If a receiving party treats their own confidential information poorly, then that is the standard to which confidential information received under the NDA will be compared to.

"

NDAs should specify how confidential information is to be used and treated.

Period of confidentiality: this issue is arguably one of the most important to cover.

4. **Period of confidentiality:** this issue is arguably one of the most important to cover. A party should consider the value of the confidential information to be disclosed and decide whether an indefinite or fixed period of confidence should be placed on it. Many NDA's are only applicable for a very limited period of time (e.g. three years). For certain types of information (e.g. financial information), that may be fine, however, for trade secrets that have lasting value, it may be woefully inadequate. An assessment as to what information you are disclosing, and how long it is likely to remain confidential, is essential.

5. **Governing law and dispute resolution:** jurisdiction is an important issue for NDAs, as the law of confidential information is subject to differing treatment from country to country. It is usually advisable to opt for a 'home' jurisdiction for familiarity, but careful consideration is necessary when dealing with parties in foreign jurisdictions, both as to the choice of law, and the format for dispute resolution. For example, an English company which obtains a judgment in the English courts against a Chinese company could struggle to enforce the same in China as the Chinese courts require reciprocal recognition for judgments, and no such agreement has been made with the UK. However, China is a signatory to the New York Convention 1958 for the recognition and enforcement of international arbitration awards. Hence arbitration (whether in the UK, China, or a neutral country) is often the preferred form for dispute resolution in NDA's with Chinese contractors, to ensure greater ease of enforcement.

Cyber security – planning for breach

Maria Peyman
Senior Associate
01223 326596
maria-peyman@birketts.co.uk

Whilst we are all now used to seeing regular reports in the news regarding the latest cyber attack, it seems that the news reports we see are only the tip of the iceberg.

In 2017 the government undertook a 'Cyber Security Breaches Survey' covering 1,523 businesses of differing sizes. A huge 46% of respondents stated that they had discovered a cyber security breach in the preceding 12 months. The most common example cited was employees receiving fraudulent emails (72%) with viruses/spyware/malware coming in as the second most commonly cited example (33%).

It is generally accepted that most organisations cannot entirely eliminate the risk of succumbing to a cyber-attack, but there are certainly steps that can and should be taken to

minimise cyber risk. To ensure proper management of risk, organisations should, of course, be implementing avoidance measures but, equally importantly, must also ensure they have a tried and tested breach management plan in place should they fall victim to an attack.

“... organisations should ... ensure they have a tried and tested breach management plan in place

Below are initial considerations to get your organisation thinking about whether it is addressing cyber security, and is broken down into five proactive steps and five reactive steps.

Proactive

1. **Assess your risk:** identify the business's valuable assets, where and how the information is stored and who has access to it. In tandem, also consider the business critical systems, for example, what would be the impact of no access to email or electronic documents?

2. **Strategy for managing incidents:** in the event of a cyber incident time is key. Every business should have a clear plan of what happens in the event of an incident and who is responsible for each action. Ensure that the plan is tested to ensure that it will work.

3. **Educate your employees:** at board level, there should be a proactive approach to cyber security as well as an overall business commitment to teaching employee awareness. To educate and maintain awareness you should produce user security policies, establish a safe staff training programme, implement effective security awareness campaigns, maintain user awareness, promote incident reporting so employees can raise issues without fear of recrimination, and make sure that you test the policies and training that you have in place.

4. **Governance and compliance:** currently laws and regulations are developed through different entities to address cyber security threats which can make it difficult for businesses to identify all of their legal and regulatory obligations. For example, if you operate in more than one jurisdiction make sure you comply with the obligations for each of those jurisdictions and, if you are a regulated entity, ensure that you comply with your regulatory body's obligations. You should also be paying particular attention to relevant data regulations.

“... ensure that you have measures in place to help protect against external and internal attacks.

5. **Network and IT security:** this may seem simple but ensure that you have measures in place to help protect against external and internal attacks. For example, establish anti-malware and firewall defences, implement intrusion and prevention and detection systems, filter malicious content and sites, and monitor and test the security in place.

Reactive

1. **Detection:** in the best case scenario, as an organisation, you will detect a cyber incident yourself. It is much worse if it is released through the media. Once detection has taken place, you need to move swiftly.

2. **Assess the cyber attack:** this is sometimes more difficult than it sounds but key early stage decisions need to be made such as notifying the regulators or, if you are a large entity or the information is particularly sensitive, managing the media. It is worth noting that cyber-attacks often happen at weekends and bank holidays which make a response more difficult as detection is less likely.

“... cyber-attacks often happen at weekends and bank holidays which make a response more difficult as detection is less likely.

3. **Containment:** once a security attack or incident has taken place, the hacker may remain ‘within’ your business’s systems and, therefore, you may choose to take compromised systems offline. You may well also want to revert to backup systems or a disaster recovery/business continuity plan if you feel that the systems are severely compromised.

4. **Investigation:** the technical investigation will be carried out by inhouse/external IT, security and forensic experts but this should all be done under the supervision of the legal team to preserve legal privilege.

   At the same time as the investigation takes place, consideration needs to be given to the legal position following the results of the investigations. For example, does the Information Commissioner’s Office (ICO) need to be notified? For regulated organisations, does there need to be a notification to your regulator? It is worth bearing in mind that regulators want to be notified promptly – in the case of the ICO within 72 hours of breach discovery.

“... consideration needs to be given to the legal position following the results of the investigations.

5. **Review:** at the end of an investigation once you are clear that the cyber incident has been contained and dealt with, your business can reflect on the cause of the breach and identify the remedies that will prevent the same attack recurring. This is a review of both software and human actions. When you get to this point, the lessons that you learn can be taken and fed into your business’s proactive steps.

Of course the above lists are not exhaustive and there will be many other considerations and aspects which are particular to an individual business so it is key to seek advice and input from all your professional advisors.

If this subject is of interest why not come along to the CBI Cyber Security Business Insight Conference – full details can be found in the ‘One for the diary’ on page 17, or visit the CBI’s website.

The regulation of cryptocurrencies

Georgina Perrott
Solicitor
01223 326635
georgina-perrott@birketts.co.uk

Virtual currencies have generally existed unregulated since Bitcoin's creation in 2009. Since then they have increased in popularity and the number of different cryptocurrencies has expanded to over 1,300 different virtual currencies.

This growth in popularity, coupled with price volatility and concerns about criminality, has led to a focus by regulators worldwide on whether, and how, to regulate cryptocurrencies. Recent news stories such as the $500m security hack of Coincheck, the Japanese crypto exchange house, highlight the need for such regulatory attention. This article considers the benefits and uses of virtual currencies, their risks and upcoming regulation.

Uses and benefits

Currently cryptocurrencies are mainly used for private transactions, raising funds via initial coin offerings and making purchases. Certain websites including Overstock, Expedia and Shopify already accept virtual currencies and others are likely to follow as cryptocurrencies become increasingly mainstream. An innovative development in the virtual currency realm is websites offering users, as an alternative to viewing adverts, the option of allowing the website to use their device to mine cryptocurrency whilst the user is using their website.

Certain websites including Overstock, Expedia and Shopify already accept virtual currencies and others are likely to follow.

The principal benefits to using cryptocurrencies include privacy, speed, low transaction costs and security. The pseudonymous quality of virtual currencies gives its users a level of privacy not afforded by 'real' currencies. This can be of real benefit in certain circumstances, for example to operate outside the confines of oppressive governments. Cryptocurrencies have lower transaction costs, and are often faster, than electronic payments made via banks. This makes them popular with users, one such group being immigrants sending remittances to their families overseas. The security of cryptocurrency transactions is a further benefit. They cannot be easily counterfeited and transactions cannot be reversed.

Risks

There is concern among regulators that cryptocurrencies are increasingly being used for illegal purposes.

The flipside to the above is that virtual currency use also presents a number of risks. Whilst privacy can be a benefit, it can mask criminal activities such as fraud, money laundering, financing terrorism and tax evasion. There is concern among regulators that cryptocurrencies are increasingly being used for illegal purposes.

The current lack of regulation leaves individual users exposed to price volatility and financial loss...

The current lack of regulation leaves individual users exposed to price volatility and financial loss resulting from operational and security failures arising at crypto exchanges. Earlier this year Lloyds Bank and Virgin Money responded to this risk by banning their customers from using their credit cards to purchase cryptocurrencies. Facebook has also decided to ban all adverts for digital currencies from its site on the basis they frequently mislead consumers.

There is also concern among some legislators that cryptocurrencies pose a systemic risk; that if the virtual currency economy continues to grow uncontrolled, it may destabilise the traditional financial system.

What regulatory approach is being taken?

The FCA has warned consumers of the risk of fraud in respect of cryptocurrencies and the dangers of initial coin offerings.

The presence of these risks and the growth in popularity of cryptocurrencies has meant governments and central banks are turning their attention to virtual currency regulation. Government responses globally range between all out cryptocurrency bans, issuing warnings only, introducing regulation and creating state-backed cryptocurrencies.

To date, involvement of UK regulators has been limited to issuing cautionary statements. The FCA has warned consumers of the risk of fraud in respect of cryptocurrencies and the dangers of initial coin offerings.

Looking ahead, the UK government is currently working with the EU to bring cryptocurrencies within existing anti-money laundering and counter-terrorism financial legislation. 'Virtual currency exchange platforms' (professional exchange houses) and 'custodian wallet providers' (the equivalent of a bank or payment institution offering a payment account) will be brought within MLD4, meaning they will need to comply with regulatory obligations including performing customer due diligence and reporting suspicious transactions. These changes are intended to crackdown on the use of cryptocurrencies for illegal activities and tax evasion.

The proposed legislation is due to come into effect at the end of 2019. Its implementation is unlikely to be affected by Brexit as the UK is expected, at least temporarily, to stay within the single market post-Brexit, and will, therefore, need to transpose the regulations into UK law.

CryptoUK has produced a code of conduct for its members which includes guidelines around better due diligence.

In addition to government regulation, there is nascent self-regulation within the UK cryptocurrency industry. Seven large crypto companies have recently set up CryptoUK, the first UK cryptocurrency trade association with the aim of improving industry standards and engaging policymakers. CryptoUK has produced a code of conduct for its members which includes guidelines around better due diligence, and ensuring customer funds can pay out in the event of insolvency and increased account security.

The future

We are currently in a period of regulatory change and it will be interesting to see what approach is taken by other countries. Governments will need to take a balanced approach to ensure technical innovation surrounding cryptocurrencies are not stifled by onerous new regulations. The borderless nature of virtual currencies means that, ultimately, a globally co-ordinated approach will be needed to create effective regulation, and governments will need to work together in the future to achieve this. This sentiment has been echoed by the IMF which has called for global coordination on the regulation of virtual currencies.

Employing EU nationals – what's the deal and what should employers be doing?

EU nationals play an important role in the UK workforce, particularly in the technology sector.

Clare Hedges
Senior Associate - Head of Immigration
01223 326605
clare-hedges@birketts.co.uk

We know employers are concerned about how best to retain their existing employees and whether their ability to recruit in the future will be hindered.

Short term

Although we will leave the EU at 11pm on 29 March 2019, there is a proposed deal which envisages a transition period until 31 December 2020. EU free movement rights would continue in full until this date and employers would be able to recruit EU nationals as normal until then.

> *Any EU nationals who are living in the UK lawfully before 31 December 2020 will be allowed to remain here.*

Any EU nationals who are living in the UK lawfully before 31 December 2020 will be allowed to remain here. They will need to document their stay by 30 June 2021. The government has published details of a new settlement scheme, which is based on residence, rather than exercise of EU Treaty rights. For more information on this scheme please see EU settlement scheme – FAQs.

Whilst the government is encouraging EU nationals to wait for the new scheme to be launched in March 2019, many are still choosing to apply for a permanent residence card now. This may be because they wish to become British citizens before we leave the EU.

In which case, under current naturalisation rules, they are required to hold a permanent residence document first. It is possible for permanent residence cards to be backdated, whereas this will not be permitted under the settled status scheme.

Medium/long term

From 1 January 2021 a new immigration system will be in place, however, we still don't know what this will look like.

From 1 January 2021 a new immigration system will be in place, however, we still don't know what this will look like. The government's white paper regarding an Immigration Bill has been delayed, and at the time of writing, this article has still had not been published.

However, we do now have a report from the Migration Advisory Committee (MAC), which makes recommendations to the government regarding immigration policy. This suggests that there should not be special treatment for EU nationals, although this may be included in any future trade deal. The MAC is in favour of high (and possibly even medium) skilled immigration, subject to certain minimum pay thresholds, but suggests low skilled and low paid immigration should be curtailed.

Many roles in the technology sector are recognised as being highly skilled and, generally, competition for staff means pay rates are high. Therefore, it seems likely that these roles will qualify for visas under the new regime.

Employers are likely to be pleased with the MAC's suggestion that the bureaucratic Resident Labour Market Test process should be abolished or reduced. However, there are likely to be budget concerns regarding the prospect of having to meet visa costs for a higher percentage of staff. Even if individuals are asked to pay for their own visa and Immigration Health Surcharge, the sponsoring employer would still need to pay the Immigration Skills Charge as is currently the case for non-EU nationals. For medium/large employers this is £1,000 per year of the visa.

What to do now

The priority must be to ensure that your existing workforce knows they are valued and that you wish to retain them. Employers do, however, need to be careful about any guidance they provide. This is because immigration advice is regulated and it is an offence to provide immigration advice if you are not qualified to do so.

A good start would be to share this article and to point employees to the wealth of information available online, including the government website.

If you wish to go further, then you may be interested in the in-house seminar we offer, which provides information to EU nationals about what is happening, what their options are, explains what we would do in certain typical situations, and sets out in generic terms how the new settled status scheme works and how to apply for permanent residence and naturalisation as a British citizen.

Employers should consider whether they would support employees with the cost of the applications required to secure their status in the UK...

Of course, we also offer individual advice as appropriate. This can range from analysis of someone's situation if they have a more complex case, to preparing applications on their behalf, to a simple checking service, for those who wish to reduce costs and prepare their own application but would like the comfort of knowing everything is in order before they apply.

Employers should consider whether they would support employees with the cost of the applications required to secure their status in the UK, or perhaps with loans if appropriate. Applications for permanent residence and the new settled status cost £65 per person. The fee for naturalisation is £1,330. Before applying for naturalisation employees will need to have passed the 'Life in the UK' test, which costs £50.

Prudent employers will also be conducting a workforce modelling exercise to consider their future needs and how these might be met:

- are increased budgets required for relocation costs?
- are there current employees who should be encouraged to develop existing skills?
- is there scope to use the apprenticeship levy to train more apprentices?

Prudent employers will also be conducting a workforce modelling exercise...

In particular for the technology sector – does all of the work need to be done in the UK or would agile working allow recruitment of new staff based abroad? If so, how would that be managed and what are the tax and social security implications?

The most creative employers will also be making sure they understand what other visa options might be available to their staff. There is a particular route: Tier 1 Exceptional Talent, which is designed to bring digital technology talent to the UK, by obtaining endorsement from Tech Nation. This scheme is still underused and employers in the technology sector should consider if it might apply to their prospective recruits. Those who get to grips with it now are likely to have an advantage in the fight for future tech talent.

For advice on this scheme and any of the other matters covered in this article, please contact Clare Hedges, Head of Immigration at Birketts.

ICO grants programme

Nicola Gulrajani
Solicitor
01603 756568
nicola-gulrajani@birketts.co.uk

The ICO grant programme is intended to fund research into privacy and data protection issues affecting the UK public.

Under the scheme, there is funding available of up to £100,000 to fund projects which will have a direct benefit to the UK public.

Previous projects funded include:

- a digital tool to help people enforce their data protection rights
- an online tool to evaluate the risk of re-identification of pseudonymised data
- research into the secure sharing of medical information and supporting research
- research into issues related to children's online privacy.

So far there have been two rounds of funding (the second round has recently closed and applications are being assessed) and it is anticipated that there will be at least two further rounds of funding available.

Based on previous years, the application window for the third round of funding is likely to be in July or August 2019. If your organisation is in the planning stages of a project which will consider UK privacy issues, now may be a good time to consider whether the project may be eligible for an ICO grant.

Who is eligible for funding

Grants are available to a wide range of organisations including (but not limited to) academic institutions, organisations with a genuine commitment to public benefit outcomes, trade and industry associations, and civil society groups. The organisations can be UK based or international, but the research must have a direct benefit to the UK public.

Political and religious organisations, current or former employees of the ICO, and anyone who has been disqualified as a director, subject to insolvency or bankruptcy proceedings, or the subject of any enforcement proceedings by the ICO, will not be eligible for funding.

What types of research are covered

The ICO is looking to fund projects which will assist it in working towards its five strategic goals, which are:

1. increasing the public's trust and confidence in how data is used and made available
2. improving standards of information rights practice through clear, inspiring and targeted engagement and influence
3. maintaining and developing influence within the global information rights regulatory community
4. staying relevant, providing excellent public service, and keeping abreast of evolving technology
5. enforcing the laws the ICO helps shape and oversee.

There was also a focus on AI, big data, machine learning, blockchain, and issues relating to the use of children's data.

For the first two rounds of funding, the ICO particularly sought solutions to implementing privacy by design and accountability. There was also a focus on AI, big data, machine learning, blockchain, and issues relating to the use of children's data. In 2018/2019 there was also a focus on safeguards in the use of biometric and facial recognition data, data trusts, and challenges for SMEs. These seem likely to remain key issues for the following round of funding.

In the majority of cases, funding will be capped at £100,000 and last for 12 months, however, the ICO does have discretion to award a higher sum or extend the time period if it believes that the project is of sufficient complexity and importance. If you know that your project may take longer than 12 months or require more than £100,000 to complete, you must explain why and justify this in your application. Extended funding is very unlikely to be granted retrospectively, unless there are exceptional or unforeseen circumstances.

What costs are covered by the grant

The grant is intended to cover the direct costs of carrying out the project such as salaries, administrative costs, reasonable travel costs and minor equipment which are required for the project (such as software).

The ICO will not fund general overheads, equipment which costs over 25% of the sum awarded, or any costs incurred before or after the funding period.

As the grant is a source of public funding, the results of your research must be made available to the public free of charge.

Can organisations commercialise the results of their research?

The ICO will not fund research which is for commercial purposes. As the grant is a source of public funding, the results of your research must be made available to the public free of charge.

Based on previous years, the application window for the 2019/2020 round of funding is likely to be in July or August 2019.

How and when to apply for the next round of funding

Based on previous years, the application window for the 2019/2020 round of funding is likely to be in July or August 2019.

You will need to send the ICO your completed application form, any supporting evidence, and a 500 word summary of your proposal. It is important that your application sets out a clear and detailed methodology, explains the project deliverables and outcomes, and provides key milestones and timescales. The application form and guidance from the 2018/2019 round of funding are available on the ICO website.

When assessing your proposal, the ICO will consider the overall quality of the application, how relevant the proposal is to the Strategic Plan, the feasibility of the project, whether it provides value for public funding, and whether it sets out clear outcomes and benefits focussed on UK data protection issues.

Deal focus

The following are examples of some of the transactions Birketts has handled within the sector in recent months.

Ventrica Limited

Birketts has advised Ventrica and its owner, Dino Forte, since its beginnings. Southend-based Ventrica is an award-winning outsourced contact centre, which provides intelligent, multi-lingual and omni-channel outsourced customer service to a range of blue-chip clients. Over the years Ventrica has become a key employer in Southend and in 2017 the company launched a second site in the town. With support from Mobeus, the company plans further investment to expand its footprint in the UK and Europe to support its growing multi-lingual client base that serve customers across global markets. However the strategy is to remain medium-sized.

Throughout the process Birketts has demonstrated a clear understanding of our business and their market knowledge showed.

In relation to the recent investment, Birketts advised Ventrica and Dino Forte on all legal matters. Adam Jones (Corporate Partner) led the team which included Alex Forwood (Corporate), Ozan Zorba (Corporate), Clare Barlow (Employment), Matthew Grindley (Property), Karl Pocock (Corporate Tax) and John Kahn (Corporate Tax).

Dino Forte, Ventrica CEO, added, *"Throughout the process Birketts has demonstrated a*

clear understanding of our business and their market knowledge showed. They have been invaluable in helping to secure investment from the right PE house in order to realise our ambitions, with their PE experience giving me confidence in negotiating the terms. With Mobeus as a partner, we are well positioned to strengthen our team to support our significant growth whilst also allowing us to better focus on our existing clients."

Adam Jones said: *"Given our long and continuing history with Ventrica we were delighted to spot this opportunity for Dino and assist him in the securing this multi-million pound investment from Mobeus. This deal required thorough knowledge of our client's business and its priorities as well as drawing upon our connections and recognising suitable investment opportunities for PE houses."*

NotSoSecure Global

Birketts advised the shareholders of NotSoSecure Global group on its sale to Claranet Group for an undisclosed sum.

Founded in Cambridge, with operations in India, US and UK, NotSoSecure is a specialist IT security firm delivering high-end IT security consultancy and training. Over the years the technology firm has become globally recognised in the field of penetration testing and hacking training.

Birketts, led by Adrian Seagers, advised on all legal matters providing Corporate, Employment and Corporate Tax advice to the shareholders, as well as working closely with Indian counsel.

"Birketts has become increasingly active in the tech space and is one of only a very few firms in the East of England that is capable of completing a transaction of this nature.

Dan Haagman, Commercial Director of NotSoSecure, said: *"Birketts has become increasingly active in the tech space and is one of only a very few firms in the East of England that is capable of completing a transaction of this nature. Birketts previously acted for me on the sale of another business, so I knew we had an excellent team advising us."*

"This transaction demonstrates once again how Birketts has highly-skilled personnel capable of delivering complex international transactions of this nature," said Adrian Seagers, Partner and Head of Birketts' Corporate Services division.

Innova Systems

Birketts and financial advisers Grant Thornton have advised the shareholders of Innova Systems UK Limited on its sale to Visiativ SA.

Established in Cambridge in 2002, Innova Systems is one of the leading distributors of Dassault Systèmes' SOLIDWORKS solutions (a 3D mechanical design software package) in the UK.

Visiativ has acquired 100% of the capital of the company. Mark Bradford, CEO and co-

We are grateful to Birketts for guiding us through this process with patience and clarity and explaining unchartered territory with clear communication and calmness.

founder of Innova Systems, will remain in office and help Visiativ to successfully integrate the company and develop other aspects of its business in the UK.

Birketts advised on all legal matters with James Allen leading Birketts' Corporate Team. Further legal advice was provided by the Tax (John Kahn), Employment (Josie Beal) and Property (Dwight Patten) teams. Additionally, Oliver Crichton acted for Innova in respect of leases/tenancy arrangements.

Mark Bradford, CEO and co-founder of Innova Systems, said: *"We are grateful to Birketts for guiding us through this process with patience and clarity and explaining unchartered territory with clear communication and calmness."*

James Allen, Corporate Partner at Birketts, added: *"It was a pleasure to guide Innova Systems' management team through the process and secure a successful integration into the Visiativ group."*

PSI Services

Birketts advised the shareholders of PSI Services (UK) Ltd on its purchase of learndirect's eAssessment business.

Learndirect is recognised as one of the UK's foremost online learning providers and this acquisition marks the latest phase in PSI's continued rapid growth in the UK and EMEA.

Under the deal, PSI, which has its International headquarters in Cambridgeshire, will take over learndirect's UK test centre network, technology and call centre along with all associated staff. PSI will also take over full management responsibility for the delivery of two extremely high profile key government programmes, including delivery of the British Citizenship Test, that PSI now deliver on behalf of the Home Office.

The quality and professionalism that we received from the legal teams at Birketts was exemplary.

Birketts advised on all legal matters with James Allen leading Birketts' Corporate Team and assistance being provided by Corinne Spencer. Further legal advice was provided by the Tax, Employment, Immigration and Property Teams at Birketts.

Janet Garcia, President of PSI's International division, commented: *"The quality and professionalism that we received from the legal teams at Birketts was exemplary. This was a complex deal that needed to turnaround in a compressed timeframe. This transaction required us to utilise their expertise across a number of specialisms, and it was incredibly useful to have those co-ordinated so efficiently. I am grateful to James and Corinne for the commitment and sound advice during the process."*

James Allen, Corporate Partner at Birketts, added: *"We are delighted to have helped to secure a key acquisition for PSI's management team and look forward to seeing the firm continue to thrive."*

One for the diary

Birketts is delighted to be sponsoring the CBI Cyber Security Business Insight Conference on 19 October, which will held at the Granta Centre located on the outskirts of Cambridge. The event is also sponsored by event partners TWI, BT and Barclays.

"Four in ten UK chief executives believe a cyberattack on their business is now a case of 'when' and not 'if'...

Four in ten UK chief executives believe a cyberattack on their business is now a case of 'when' and not 'if', according to a recent survey of UK business leaders and chief executives.

This conference brings business leaders face-to-face with some of the UK's foremost industry experts on cyber security, including representatives from Anglian Water Group, BT, Softwerx, Barclays, Birketts and The National Cyber Security Centre (NCSC). The CBI's Director of Innovation will also provide the latest intelligence and policy insight from government, while considering business impact.

Through in-depth plenary presentations and panel discussions our expert contributors will provide inspired thinking and practical solutions to enable you to plan your strategy with confidence.

Join us to hear more from experts and industry peers on subjects such as:

- cyber-breach and the risk to brand reputation and customer trust
- empowering your employees with the skills and behaviours to make them your strongest defence
- investing and managing cyber security on a budget
- how to prepare and respond to a cyber attack
- understanding the changing threat-landscape.

To book your place, please visit the CBI's website.

Best Employers Eastern Region – congratulations

In the first edition of Upload we reported on the launch of the Best Employers East Region 2018.

We are now delighted to reveal that the winners of the 2018 programme were announced during an awards conference on 3 October.

Our congratulations go out to all winners and businesses achieving accredited status. Special mentions go to Aramar Solutions which secured platinum accreditation and winner of the award for best overall small company, and to Purple Tuesday, Riverlite, Solarflare and Tiger Eye Consulting which all achieved the gold accreditation standard.

“Our congratulations go out to all winners and businesses achieving accredited status.

Jeanette Wheeler, partner at Birketts, commented: *“Birketts has been thrilled to be part of this journey and I have been hugely inspired over the years by being part of the scheme.”*

A full list of 2018 winners can be found at www.edp24.co.uk/business/best-employers/our-members.

To find out more about Best Employer Eastern Region and sign up for the 2020 program please visit www.edp24.co.uk/business/best-employers.