Spirit
Experience
Solutions
Expertise
Talent
Know-how
Thinking
Doing
Insight
Enthusiasm

Higher Education Bulletin

April 2016

AHUA

SHAKESPEAREMARTINEAU

Contents

Register of people with significant control - does it apply to your university and subsidiaries?

With the turn of the financial year many universities have asked whether they, or their subsidiary trading companies, have to keep a Register of People with Significant Control (PSC).

The requirement to keep a Register was introduced by the Small Business, Enterprise and Employment Act 2015, amending the Companies Act 2006 by inserting section 21A. From 6 April 2016, companies, Societas Europaeae and Limited Liability Partnerships will, in addition to keeping a register of members and directors, have to keep a register of individuals or legal entities that have significant control over them. This information has to be filed annually by 30 June at Companies House in a Confirmation Statement, which replaces the Annual Return from June 2016.

Section 21A of the Act is a 'statutory trail' that must be worked through to discover whether a company must keep the Register. Companies must register any 'registrable individual' or 'registrable relevant legal entity' that has significant control over them – these terms, and what constitutes significant control, are defined in the Act. Those with significant control include those that: directly/indirectly hold more than 25% of the shares or voting rights; directly/indirectly hold the right to appoint or remove a majority of directors; or otherwise have the right to, or actually exercise, significant control over the activities of the company or, in certain circumstances, trust or firm without legal personality (e.g. English Limited Partnerships).

The first piece of good news for many universities is that if they are a statutory or chartered body as many are, and therefore not a company for the purposes of the Companies Act 2006, they are not subject to the requirement to keep a PSC themselves. However, other universities or HEIs taking a different legal form may be subject to the requirements, particularly those that are private companies.

Many universities which are statutory and chartered bodies will have wholly owned trading subsidiaries which they use to transact commercial business. These companies will usually take the form of Companies Act companies, usually companies limited by shares, and will therefore have to keep a Register of PSC themselves. But what should such companies record in their Register? Are there any 'registrable individuals' or 'registrable relevant legal entities' in relation to these wholly owned subsidiaries? When their owners are statutory or chartered bodies the answer to this question will usually be no. Statutory/chartered bodies are clearly not capable of being 'registrable individuals', but neither are they 'relevant' legal entities, as they are not 'subject to their own disclosure requirements' as required by the Act for a 'relevant' legal entity. So, the wholly owned subsidiary company of a statutory/chartered corporation must keep a PSC register, but it may enter the phrase "The company knows or has reasonable cause to believe that there is no registrable person or registrable relevant legal entity in relation to the company" (as suggested by BIS guidance Register of People with Significant Control – Guidance for Companies, Societates Europaeae and LLPs).

Any university that has 'chains' of companies however (e.g. a wholly owned subsidiary company that then owns further companies) may find that those further down the chain are required to enter something further in their

Register of PSC than the above sentence: clearly each university should take legal advice about its individual position, and the position of its subsidiary companies, in relation to the requirement to keep a Register.

However, there is some leeway in the requirement to keep a PSC Register at present, in that those companies which were required to keep a Register from 6 April may, whilst making enquiries into who has significant control over them, enter the phrase "the company has not yet completed taking reasonable steps to find out if there is anyone who is a registrable person or a registrable relevant legal entity in relation to the company" in their Register until such (reasonable) time that they have taken such steps.

The important thing is that a Register must have been in place from 6 April and the information contained within it sent to Companies House in your Confirmation Statement by 30th June. Failure to do so will be a criminal offence.

Hester Fairclough
Paralegal, Education
T: 0121 214 0565
E: hester.fairclough@shma.co.uk

Cybersecurity Part III: The Battle of Apple v America

The stand-off between Apple and the US government around demands from the latter to access an iPhone has come to an end. As a quick reminder, the US government wanted Apple to create a "back door" to unlock the iPhone owned by Rizwan Farook, the man who, together with his wife, shot 14 people last December. In the end the FBI managed to get into the phone and now won't tell Apple how they did, potentially allowing them to access any iPhone.

This is not the first time there have been requests by US government agencies to access personal communications. As the final part of our overview of cybersecurity, we will consider the implications of arguably legitimate reasons to access personal data and communications on wider data security.

It might seem a no brainer: why would Apple not allow access to the phone of one of the attackers in a mass shooting, particularly as it might contain data on the 'Islamic State' group? However, Apple refused to comply with the court order. Tim Cook, Apple's CEO, argued that giving the FBI this software would be "dangerous" and "chilling". He said that allowing access to this data would leave it vulnerable to exploitation by governments and criminals and potentially lead to flinging wide the floodgates for data requests. Sceptics would also argue that Apple's defiance is not surprising in light of documents leaked by Edward Snowden a few years back claiming that Apple, amongst others, gave access to sensitive information to the security agency. Now that the FBI have found a back door to Apple iPhones, the company will need to firstly work out how they got in before finding a solution.

Despite perhaps appearing a distant problem, the outcome of this ongoing saga could have several potential implications for UK universities. Whether or not Tim Cook's concerns around snowballing governmental requests and ultimately access to personal data is an exaggeration, the line between the right to individual freedoms and the governmental need to protect national interests is often a blurred one. The obvious concern for universities is that, with government access to potentially unlimited data, the checks and balances that would normally restrict access will not be sufficient. Given the UK's history of surveillance – we have one of the highest numbers of surveillance cameras in the world - it could be a worryingly short step for the UK to follow America in demanding increased access to private communications.

Concerns around the use of data in the US are not new. Data protection laws in the UK and the EU are strict, particularly in relation to sending data outside of the EU. After the European Court of Justice ruled that the 'Safe Harbor' principles that allowed US companies to comply with EU privacy laws are no longer sufficient, new draft legislation is in circulation. However, even with this in place the Apple dilemma raises further concerns around protecting data outside of the EU.

In previous articles we have discussed the serious nature of the threat of cyberattacks and the impacts these attacks can have on universities. To some extent, Tim Cook's concern that offering software access to hack into phone data could make individual communications more vulnerable to criminal activity is probably a fair one. Universities will be aware that even within their organisations, limiting access to data and ensuring that staff comply with policies to protect that data is crucial in complying with their obligations. Apple will be aware that it won't just be the government that can bypass Apple security, which raises the question of how secure are iPhones from attack. Moreover, governmental security is not impenetrable and any data breach has wider-reaching consequences, so creating a direct entry point to currently secure personal data, although only intended for use by the US government, could have drastic implications following a successful cyberattack. This is

another area of concern for Apple about access to their phones.

If the government is keen to have access to personal communications, it is no real surprise that businesses can also find the lure of profitable data irresistible. Students at the University of California-Berkeley are currently suing Google, which runs the University's email accounts, for illegally scanning their emails for commercial purposes without the students' consent. Advertisement scanning is nothing new, but the complaint alleges that the scanning took place after the company had announced it had permanently removed all advertisement scanning. The outcome of this case may be of considerable interest for UK universities that use a similar service and may have been potentially exposed to a similar situation. Universities probably have measures in place in their contracts already, although the draft General Data Protection Regulations look to extend these further and so universities may want to consider reviewing them in light of this when they come into force.

The Apple debate demonstrates that cybersecurity issues are not as straightforward as they may initially seem, and the changing landscape of data access makes keeping abreast of issues difficult, but essential. Despite concerns, the same practical steps that have been mentioned previously can help universities comply with their obligations. Clear policies for staff who process data, that are user friendly, properly implemented and managed, and the provision of refresher training where necessary, are essential in protecting against breaches. With the rise of cyberattacks alongside the development of more advanced technology, no protection will ever be able to prevent all cyber attacks, but as a key institutional risk, cybersecurity is a crucial consideration for organisations worldwide.

Lydia Stone-Fewings
Trainee Solicitor, IP & Commercial
T: 0121 214 0315
E: lydia.stone-fewings@shma.co.uk

No more HMOs

On 13 April 2016 the Multiple Occupation (Specified Educational Establishments) (England) Regulations 2016 came into force. These change the law in relation to Houses in Multiple Occupation (HMOs).

The new legislation provides that any building which is managed or controlled by an education establishment (e.g. a university) and which is occupied solely by students engaged in full time education will not be considered as an HMO. As a result of this change, universities will no longer be required to apply for the relevant licences for a property to be deemed as an HMO.

This will be a welcome introduction for universities which, under the current rules, are required to apply for several licences in order for properties to be deemed as HMOs.

Universities will also no longer be liable to be fined £20,000 for failing to hold the correct licences. This is provided that they can show, if required, that the majority of occupants within the property are full time students only at the relevant establishment. Given the recent increases in prosecutions for failing to obtain correct licences this will also be good news for universities.

Whilst it will no longer to be necessary to hold the relevant HMO licences, universities will still be required to comply with various health and safety standards. This is to ensure that HMOs are of an acceptable health and safety standard in light of multiple occupants residing within the property. As such, universities should continue to carry out inspections and any other health and safety processes they adopt to ensure compliance and to identify any property defects, and remedy any problems found soon as possible.

Justine Ball
Solicitor, Real Estate
T: 0121 214 0306
E: justine.ball@shma.co.uk

April 2016 changes - get ready!

There are a number of employment law changes coming into effect in April 2016. A summary of the key changes is set out below:

- A significant development for lower paid workers is the introduction of the National Living Wage. From 1 April 2016, all workers aged 25 and over will be entitled to at least £7.20 per hour.
- From 6 April 2016, a new scheme will penalise employers who fail to pay tribunal awards or settlements agreed via ACAS. The penalty will be 50% of the unpaid sum, subject to a minimum of £100 and a maximum of £5,000. If the employer pays both the unpaid sum and the penalty within 14 days, the penalty will be reduced by 50%.
- For tribunal claims issued on or after 6 April 2016, new tribunal rules will introduce a deadline for making postponements of seven days before the hearing, as well as limiting the number of postponements to two for each party. Tribunals will be required to consider making a costs order or a preparation time order against a party who makes an application to postpone or adjourn less than seven days before a hearing.
- For dismissals on or after 6 April 2016, the maximum compensatory award cap for unfair dismissal will increase from £78,335 to £78,962 and the maximum amount of a week's pay (which is used to calculate statutory redundancy payments and various other awards) also rises from £475 to £479.
- A single-tier state pension replaces the current basic state pension and second state pension with a flat-rate payment from 6 April 2016 (to apply to retirements from that date). The ability for employer schemes to contract-out on a salary-related basis (by providing alternative benefits outside of the state pension) will disappear.
- Rules requiring certain public sector employees to repay exit payments where they return to work in the same part of the sector within 12 months are expected to come into force in April 2016.

Rachel Parkin
Associate, Employment
T: 0121 214 0109
E: rachel.parkin@shma.co.uk

Tempted to pull a sickie?

We hope not!

The Employment Appeal Tribunal has found that an employee who 'pulls a sickie' is in fundamental breach of contract and is therefore liable to be dismissed for dishonesty *(Metroline West Ltd v Ajaj (UKEAT/0185/15/RN)*).

This is a decision that the vast majority of employers will understand, agree with and welcome, although it has taken the appellate tribunal to clarify the position. It also leaves employees in no doubt as to the potential consequences of pretending to be ill when they are not.

Facts of the case

Mr Ajaj was a bus driver for Metroline. He suffered an injury at work, following which Occupational Health deemed him not to be fit for work for a significant period of time. However, Metroline had concerns about whether Mr Ajaj's injuries, and their impact on his health and mobility, were genuine. As a result Metroline placed Mr Ajaj under covert surveillance and upon reviewing the footage, Metroline believed that there was an inconsistency in the reporting of Mr Ajaj's injuries.

Metroline then invited Mr Ajaj to a disciplinary hearing, following which he was dismissed on the grounds that he had made a false claim for sick pay, had misrepresented his ability to attend work and had made a false claim of an injury at work.

However, when Mr Ajaj brought a claim of unfair dismissal, his claim was upheld by the Employment Tribunal, the judge finding that the employer could have had no reasonable belief in the allegations and had failed to conduct as much investigation as was reasonable.

The judge also found that a reasonable employer would have considered Mr Ajaj's medical position and decided whether to continue his employment against an assessment of capability.

The Employment Appeal Tribunal overturned the Tribunal's finding, deciding that the Tribunal had substituted its own view for that of Metroline, and that the dismissal was therefore fair in the circumstances. It found that Metroline did have a genuine and reasonable belief, based on reasonable investigation, that Mr Ajaj had attempted to commit fraud or at least to misrepresent and exaggerate his symptoms.

The Employment Appeal Tribunal concluded: *"An employee [who] 'pulls a sickie' is representing that he is unable to attend work by reason of sickness. If that person is not sick, that seems to me to amount to dishonesty and to a fundamental breach of the trust and confidence that is at the heart of the employer/employee relationship."*

What does it mean for universities?

In the modern world of mass communication and social media postings, it's not unusual for employers to become concerned about the genuineness of an employee's absence.

The judgment from the Employment Appeal Tribunal is extremely helpful in confirming that an employer who can show, on the balance of probabilities, an employee has 'pulled a sickie', will be entitled to dismiss that employee for gross misconduct (subject, as always, to a reasonable investigation being carried out, a fair process followed and the employer having a reasonable belief in the employee's dishonesty).

Tom Long
Legal Director, Employment
T: 0121 214 0147
E: tom.long@shma.co.uk