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

Higher Education Bulletin

February 2016

AHUA

SHAKESPEAREMARTINEAU

Contents

Strategy, Students & Governance

Commercial

Estates

Human Resources

Do sanctions laws apply to your university's activities?

The Times Higher Education World University Rankings 2015-16 found that Saudi Arabia is the top performer in the Arab region; other countries given a mention in the top 15 included Lebanon, Qatar, Oman, Jordan, Egypt and Morocco. The published rankings, and the slight thawing of relations between the UK and Iran, raise the potential for increased collaboration between universities in the UK and those in the Arab world. However, many of the countries mentioned in the rankings are ones against which the UK has some kind of sanctions and/or embargos in place, and many universities already operate either student recruitment or teaching/research programmes in these countries, including Syria and Iran.

Most UK sanctions laws are aimed at restricting the flow of arms, goods that could in any way be used for the internal repression of a civilian population, and goods that support industries that fund sanctioned regimes. The oil, gas, petroleum and chemical industries are often targeted due to their role as funders of regimes in countries where such products are usually the country's most valuable natural resource.

The UK government issues notices to exporters and guidance on each listed country on the Department for Business Innovation and Skills website. It also produces a Consolidated List of individuals and entities against whom asset-freezing laws apply. Although UK individuals are also named, many of those individuals on the asset freeze list inevitably originate from sanctions-listed countries.

Whilst the recruitment of students from sanctions listed countries often poses no problems, as long as those recruited are checked against the Consolidated List, the implementation of research and/or teaching programmes can be more problematic. Many of the items listed as banned from export are technological hardware and software components and chemical agents; potential scientific and medical research programmes are the most likely to use these items and therefore are most likely to breach sanctions laws. Any programme likely to involve the gas, coal, petroleum or chemical industries in the partner country will also have to be carefully considered, given the number of prohibited actions relating to these areas.

As universities increase their collaborative activities with Arab and North African countries they should continue to check whether those activities in listed countries comply with sanctions laws.

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

From Bricks to Clicks – The HE Commission Report: Learning analytics and the use of data in shaping the future of the sector

The Higher Education Commission recently released a report "From Bricks to Clicks" which explores the implications for the HE sector of the volume of data institutions collect from and about their students.

Other than face-to-face lectures and seminars, students have multiple contacts with their institution throughout their studies: the submission of applications; enrolment itself; attendance at seminars and lectures; webinars; submission of work and receipt of feedback online; and logging in and out at university buildings such as libraries, laboratories and so on.

As a result of these actions a data footprint is left by individual students which, once collated, becomes a huge dataset. So, to what extent and in what ways does the Commission consider that universities could and should utilise this dataset?

An increasingly common use of data is learning analytics, i.e. understanding how students learn, to optimise the student experience. Motivations for the use of learning analytics include increasing retention, providing better feedback to students, capturing attendance data and enhancing teaching and learning. The analysis of data collected can also identify barriers to equal access to HE, inform future strategic planning, and potentially identify and foster excellent teaching and collect data for TEF submissions, depending on the final shape the framework takes.

However, the collection and analysis of data about individuals inevitably raises legal, ethical and practical concerns and challenges. Issues surrounding student consent for use of data, and potential breaches of privacy, are obviously problematic. The current system of data collection is described by the Commission as "overly complicated, burdensome and involves unnecessary duplication, where institutions are required to submit the same or similar data to a range of different bodies." A dearth of "data-capable" and visionary staff and a lack of resources, skills and systems within institutions (including at senior management level) are also identified as factors which make the management of data difficult. Another concern raised in the course of the Commission's inquiry was the possibility that students would "game the system", manipulating analytics in order to achieve false positive results, thereby undermining the system's credibility.

The report makes a number of recommendations to address these concerns and a future is foreseen where data can be harnessed to shape the sector's strategic planning, improving the student experience. These 12 recommendations span a number of core themes:

- Sector bodies should work together to create a landscape that facilitates excellent and innovative data management and streamlined data collection;
- Institutions should develop a strategic and systematic approach to data collection and management and to learning analytics, and develop codes of practice to address the legal and ethical considerations involved in these activities.
- University leaders and staff should have an appropriate level of understanding of the issues to perform their roles effectively in a digital, data-driven world, with training to improve their digital capability.

A copy of the report can be found **here**.

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

Key legislative developments in Commercial Law in 2016

Last year boasted some key developments in commercial law, including the introduction of the Consumer Rights Act 2015; the restatement of the penalty clause rules by the Supreme Court; the introduction of the Modern Slavery Act 2015; and the introduction of the Public Contracts Regulation 2015, which transposed into our law the Public Sector Directive. 2016 is set to be no different. Here is a summary of some key developments or events for commercial law which we can expect to see in 2016.

ODR Regulations

The Online Dispute Resolution for Consumer Disputes Regulations provide for the creation of a European ODR platform in the form of an interactive website accessible in all languages of the EU free of charge. This out-of-court system applies to any purchase made either domestically or across the EU. From 16 February 2016 online traders will be required to provide consumers with adequate information in relation to the possibility, where a dispute has arisen in relation to a contract for goods or services, of recourse to an out-of-court dispute resolution.

With regards to the Online Dispute Resolution Platform (ODRP) an online trader must now provide the following information:

- Information regarding the existence and the possibility of using the ODRP in their online goods or service contracts
- The online trader must provide a link to the ODRP on their website.
- Where an online trader is obliged by law or their trade association to use alternative dispute resolution (ADR) services provided by a specific ADR entity, then the online trader will have to include a link to the ODRP in any offers made, via email, to the consumer.

Modern Slavery Act 2015

From 31 March 2016 the Modern Slavery Act 2015 will require universities and other commercial organisations with a total turnover of £36 million or more to start preparing their annual slavery and human trafficking statements by the end of their financial year. Organisations are being encouraged by the government to publish their annual statements no later than six months after the end of their financial year.

Procurement

As part of the modernisation programme with regards to the public procurement rules the European Union created three new directives: the Concessions Directive, the Public Sector Directive and the Utilities Directive. So far only the Public Sector Directive has been transposed into UK law in the form of the Public Contracts Regulations 2015. The remaining Directives require implementation into national law by 18 April 2016.

Electronic Identification Regulation

On 1 July 2016 the majority of the provisions of the Electronic Identification Regulation (the Regulation) will come into force and repeal the E-Signature Directive, which has provided the legal basis for the current UK legislative framework governing electronic signatures (the Electronic Communications Act 2000 and the Electronic Signatures Regulations 2002). The Regulation has direct effect in the UK but will not automatically repeal the current UK legislation in this area. As a result some uncertainty remains regarding how the Regulation will take effect in the UK. Broadly speaking the Regulation makes a number of changes across three key areas of law governing online authentication: trust services; electronic identification schemes; and electronic signatures. As yet, however, much of the detail of the Regulation remains unpublished.

We will continue to keep you updated about all of these developments in future editions of this bulletin.

Carol Gunning
Senior Associate, Commercial
T: 0121 214 0533
E: carol.gunning@shma.co.uk

Danielle Humphries
Paralegal, Commercial
T: 0121 214 0580
E: danielle.humphries@shma.co.uk

Cybersecurity Part II: the mistakes of Ashley Madison

Ashley Madison, a popular dating website priding itself on offering a secure and discrete forum for organising extra-marital rendezvous, was left red-faced in the wake of a cyberattack that exposed details of over 30 million accounts. Worryingly, senior members had raised concerns about a lack of security awareness across the organisation prior to the breach, and it was revealed that credit card details, addresses and more intimate data had limited security protection. In last month's bulletin we discussed why cybersecurity is a hot topic, the risks associated with it and practical means of protection. This month we will take a closer look at the obligations placed on universities by both current and proposed EU legislation to aid cybersecurity protection, and how to ensure compliance.

The big hitter is the Data Protection Act 1998, which places cybersecurity obligations where personal data is processed or collected. Data controllers must take appropriate technical and organisational measures which proportionately balance the state of technological developments and cost of implementation, and account for the potential resulting harm and the nature of the data. As demonstrated by PricewaterhouseCooper's (PwC) recently published report (see below), people can be a challenge to cybersecurity, and this is dealt with in the legislation by requiring organisations to ensure the reliability of their staff with access to personal data, and, where outsourcing occurs, making the data controller liable for external processing failures. Data must only be processed for its intended purposes and retained for as long as necessary, a principle poorly demonstrated by Ashley Madison, where despite being paid by customers leaving their site to remove all traces of their accounts, details from accounts that hadn't been used for well over a year were revealed by the attack.

Woe betide universities that underestimate these obligations. Enforcement by the Information Commissioner's Office (ICO) can include fines up to £500,000, and institutions face litigation claims from affected individuals and/or other organisations. With the recent estimate by TalkTalk that the attack it suffered last year cost the company £80 million and more than 100,000 customers, the potential damage is significant.

The proposed EU General Data Protection Regulation will extend these obligations and will require implementation over the next two years. In addition to ensuring processing is "by design" and "by default" i.e. limiting it to what is necessary, using it for the purpose of collation and only allowing access where essential, the proposed legislation looks set to require stricter breach notification and increase regulatory fines significantly. It will obviously be important for universities to get it right, but as current drafting stands the best preparation is to ensure compliance with the current law and to follow ICO best practice.

Additional obligations arise under the Human Rights Act 1998, requiring protection for an individual's right to private and family life, home and correspondence and freedom of expression. Litigation against institutions has been successful where personal information was obtained by staff not intended to see it, which ultimately detrimentally affected the individual. Regulated sectors are subject to additional legislation, but the proposed Electronic Identification Regulation requires universities that deal with their own trust services, including electronic identification schemes, website authentication and electronic certificates, to comply with extra security and incident reporting measures.

However, as PwC reports, nearly 9 out of 10 large organisations suffer some form of security breach, and, despite increased training, staff cause breaches just as often as viruses and malicious software. Therefore, a crucial line of defence is to ensure policies and procedures are implemented. Although it seems obvious not to click on dodgy pop-ups or emails, allow

numerous people access to staff personal information, or plug in unnecessary portable devices into organisation networks, these are common mistakes that are made and need to be included in policy drafting. Obviously, serious consideration will need to be given to technical measures to ensure adequate protection is in place, but internal housekeeping and ensuring compliance with policies and procedures will be just as important to avoid embarrassment similar to that experienced by Ashley Madison.

For more information please see:

http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html

https://ico.org.uk/for-organisations/guide-to-data-protection/

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

Clamping down (or not) on parking on private land

In England and Wales it is not now possible legally to clamp and/or remove vehicles as a result of trespass/illegal parking on private land, as the right to do so was abolished under the Protection of Freedoms Act 2012 (the Act). However, the Act has introduced an enforcement scheme which provides that the driver and/or registered keeper of a car which is trespassing/parking on private land is liable to pay parking charges. It is important for universities to be aware of the law in this area in order to preserve their right to take enforcement action against trespassers.

In summary, the scheme in the Act provides that a private landowner can seek to recover a parking charge from a driver/registered keeper of the car if s/he illegally trespasses/parks on private land and a Parking Charge Notice (PCN) is issued.

In order to issue a PCN, universities should make it clear to the public the terms upon which they can enter and park on university land by erecting appropriate signage. This signage should set out parking tariffs and/or restrictions for parking on the land and the fact that in the event such terms are not adhered to, then a parking charge will apply.

The terms of entering the private land have then been made clear to the public, and should these be contravened a PCN can be issued. It appears that £100 is the maximum that can be recovered as a parking charge and, in any event, such a sum should reflect a genuine pre-estimate of loss that the university will suffer (i.e. taking the time to issue the notice, serve this on the driver/keeper and enforce the same).

It may be that a university will choose to erect signage as a deterrent and only preserve its right to issue a PCN rather than incurring the cost and time of taking active steps to administer parking charge notices. There are statutory regulations on issuing PCNs as well as the form and content of the same which would need to be complied with if such steps are to be taken.

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

Settlement payments – what's taxable and what's not?

The recent case of Moorthy v The Commissioners for Her Majesty's Revenue and Customs ([2016] UKUT 13 (TCC)) considered whether a payment in respect of injury to feelings made on the termination of employment is subject to tax.

Facts

The claimant, a senior employee of an engineering contractor, was made redundant in 2010. Following termination of his employment, he brought claims of unfair dismissal and age discrimination. The claims were settled under the terms of a settlement agreement and the claimant was paid an ex-gratia sum of £200,000 by his employer, who treated £30,000 as tax exempt under s401 of Income Tax (Earnings and Pensions) Act 2003 (ITEPA) and deducted tax at the basic rate from the remainder.

In his tax return, the claimant treated the balance as tax free. HMRC disagreed and issued a closure notice treating an extra £140,023 as taxable income, but they did make a concession to treat a further £30,000 as damages for injury to feelings arising from age discrimination, and so not taxable.

The claimant appealed but the First Tier Tax Tribunal held that the balance was taxable. The claimant appealed again. The Upper Tribunal upheld the decision. Section 406(b) of ITEPA treats a payment "on account of injury to an employee" as not taxable, but that must relate to a medical condition. 'Injury' is akin to death or disability and does not include injury to feelings. The claimant lost the concession for the extra £30,000.

What does this mean for universities?

Universities need to be mindful of what is and is not taxable in relation to settlement payments. If HMRC finds that an employer should have deducted tax at source, liability for payment of the tax will rest with the employer. Also, although a tax indemnity in the settlement agreement may allow the university to recover the money from the ex-employee, chasing payment may be troublesome and the university may still be liable to pay penalties and interest if it is seen to be avoiding and/or evading payments of tax.

Useful reminders for universities considering the taxation of settlement payments

- The £30,000 exemption under s401 of ITEPA mainly includes non-contractual termination payments; payments for compensation for a change in job role; and compensation for a change in earnings;
- Redundancy payments (even contractual) fall within the £30,000 exemption;
- If there is no payment in lieu of notice (PILON) clause in the contract of employment, the payment can be paid free of tax (subject to the £30,000 limit). If there is a PILON clause, it should be paid subject to tax;
- Compensation for discrimination not related to the termination of employment (e.g. compensation for discrimination during employment) is not taxable;
- Contributions to outplacement counselling can be paid free of tax in most circumstances; and
- Contributions to a registered pension scheme can be paid free of tax.

Abigail Halcarz
Solicitor, Employment
T: 0121 214 0388
E: abigail.halcarz@shma.co.uk

Work emails - an unrestricted right to pry?

A recent European Court of Human Rights case (Barbulescu v Romania (61496/08 [2016] ECHR 61) has confirmed that an employer who monitored and accessed an employee's personal messages sent through a work-related Yahoo Messenger account did not breach his right to privacy under Article 8 of the European Convention on Human Rights.

Facts

Mr Barbulescu was dismissed for personal use of a Yahoo Messenger account that he set up at his employer's request to deal with client enquiries. It was alleged that he had used the account to send personal messages on his employer's computer during working hours.

Mr Barbulescu denied sending personal messages through the account. The employer therefore accessed the personal messages as part of the investigation in order to prove a breach of its rules.

Mr Barbulescu argued that:

1. his dismissal had been based on a breach of his right to privacy; and
2. his emails constituted personal data and sensitive personal data as they related to his health and sex life.

The employer had policies in place which expressly prohibited personal use of company computers. The issue was therefore whether Mr Barbulescu had a reasonable expectation to privacy when using the work Yahoo Messenger account.

The ECHR concluded that a fair balance had been struck between Mr Barbulescu's right to a private life and his employer's interests in the context of these disciplinary proceedings. It also concluded that the employer's monitoring was proportionate as no other data or documents stored on Mr Barbulescu's computer had been accessed.

What does this mean for employers?

This case does not give employers carte blanche to monitor their staff's personal emails. Indeed, this case might have been dealt with differently in the English courts, particularly in the light of the Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the fact that the employer had failed to warn the employee that internet and email monitoring was in place.

However, Mr Barbulescu had denied using the account for personal use, thus necessitating the employer's decision to access the personal emails to check the contents of those emails. The decision may have been very different if Mr Barbulescu had admitted the usage in the first place.

This case is a reminder for employers to ensure they have robust internet and e-mail policies in place covering the monitoring and surveillance of emails, messaging services and internet access on work equipment. The policy should be properly communicated to all staff to ensure that they are aware their usage is being monitored.

Any email and internet surveillance should always be proportionate. Whilst there is clearly a need for employers to be able to monitor what their employees are doing during working hours, this needs to be reasonable and balanced against the employees' right to privacy. As one of the judges in this case stated "...workers do not abandon their right to privacy and data protection every morning at the doors of the workplace."

Beverley Smith
Associate, Employment
T: 0115 945 3727
E: beverley.smith@shma.co.uk