

Regulatory Outlook

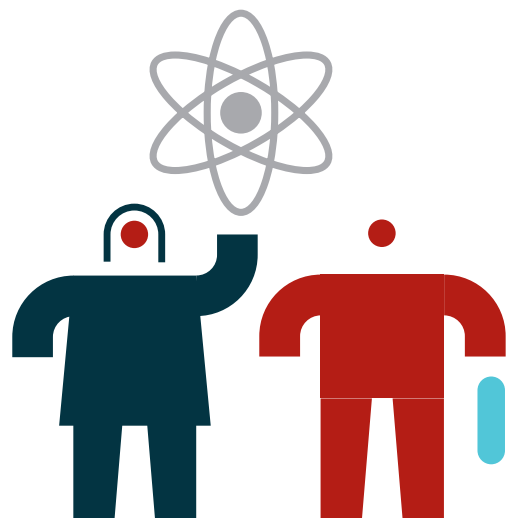
Helping you succeed in tomorrow's world

July 2017



Contents

A Message from Catherine Wolfenden	3
Advertising and Marketing	4
Anti-Bribery, Corruption and Financial Crime	6
Competition	8
Consumer Protection	10
Cyber Security	12
Data Protection and Privacy	14
Dual-Use Goods and Export Control	16
Employment and Contingent Workforce	18
Environment	20
Health and Safety	23
Product Regulation	25
Regulated Procurement	27



A Message from Catherine Wolfenden



Catherine Wolfenden

Partner and Head of Osborne Clarke's Regulatory Group

T: +44 117 917 3600

catherine.wolfenden@osborneclarke.com

A focus on personal liability

For good policy reasons, many areas of business regulation in the UK impose personal liability on directors, officers and other employees. The risk of disqualification, a personal financial penalty or even a custodial sentence is a significant influencing factor driving regulatory compliance by a corporate entity.

In this edition of the Regulatory Outlook, we examine where personal liability can be imposed under a range of regulatory regimes. A common theme is that regulators increasingly see personal liability as the most effective way of driving positive change in businesses' approach to corporate compliance. Instances of long custodial sentences are still rare, but the number of prosecutions is increasing.

Individuals within a business who could potentially have personal liability for a regulatory breach need to be aware of that risk. Compliance systems and processes must exist and be regularly tested and updated to mitigate risk of regulatory breaches and follow-on enforcement action, against both the corporate and individuals within the business. Effective compliance programmes require input from the whole of the business, not just the legal, risk and audit functions. Above all, a culture of compliance, from the top down, will be key to persuading a regulator that steps were taken to prevent regulatory breach, and may be vital in trying to protect individuals from prosecution.

Brexit

When it comes to regulation, one of the things that businesses find most challenging is uncertainty. This makes Brexit a major challenge.

Slowly the fog of uncertainty around business regulation in the UK post-Brexit is starting to recede. The Government intends to transpose all EU-derived law as at the date that the UK is due to leave the EU, in March 2019, into national law. Existing regulatory regimes should, therefore, be preserved at first, although possibly with a different regulator or institution. This will include new EU laws, such as the

General Data Protection Regulation, which will be in effect by the date that Brexit takes effect.

But for reforms that are still progressing through the legislative process, the situation is less clear. The European Commission's Digital Single Market strategy, to take one example, has been a flagship legislative initiative that we have covered extensively in this and previous editions of the Regulatory Outlook, affecting **Consumer Protection**, **Competition** and many other regulatory regimes. However, some of the strands of the DSM are some way off becoming EU law and may, therefore, not form part of UK law after Brexit. Whether the UK decides to follow the regulatory reforms that come through in the EU under the DSM could have a significant impact for businesses, whether operating from the UK into the EU or vice-versa.

While in many areas it is still too early to tell what the position will be in the UK post-Brexit, businesses that are not already doing so need to start preparing and contingency planning (if they have not been doing so already). Indeed, some regulators are actively requiring firms to provide details of the steps they have taken to prepare for Brexit.

In order to be able to undertake this exercise, now more than ever, businesses need to ensure they have an understanding of the areas of regulation that affect them. This Regulatory Outlook is intended to help with this, focusing on the areas of regulation that are most likely to be relevant to businesses in the UK, in whatever sector you operate.

How can we help?

This Regulatory Outlook draws on the expertise of over 40 regulatory lawyers in Osborne Clarke's UK Regulatory Group. Whether you are interested in personal liability, a specific development covered in this Regulatory Outlook, or would welcome a wider discussion about regulatory compliance or how you can prepare for Brexit, please do get in touch with me, the relevant expert for the area you are interested in, or your usual Osborne Clarke contact.

Advertising and Marketing



Nick Johnson

Partner

T: +44 20 7105 7080

nick.johnson@osborneclarke.com

Current issues

Brexit and advertising regulation

Regardless of what the final Brexit deal looks like, it seems unlikely that advertising regulation will change significantly in the short to mid-term. The Committee of Advertising Practice is on record as saying there are unlikely to be any changes in the short term to the Codes ruled on by the Advertising Standards Authority (ASA) or to the ASA's overall regulatory activity. However, there are certain areas of European law where some advertisers might hope to see a new approach post-Brexit. One is in the area of comparative advertising, where the doctrine of 'riding on the coat-tails' potentially helps entrench the position of dominant market players to the detriment of challenger brands. Another is in the area of health and nutrition claims relating to foods, currently regulated under an EU Regulation, which has caused considerable frustration for many food and drinks advertisers.

ePrivacy Regulation

The European Commission's proposal for updating the ePrivacy Directive was published on 10 January 2017. The legislation is drafted as a Regulation and, since it aims to sit alongside and be consistent with the GDPR, the proposal aims for the Regulation to come into force on the same day as the GDPR (25 May 2018). It is still in draft form and may change before it is approved by the European Parliament. However, as currently drafted, the Regulation would introduce significant changes in relation to cookies and direct marketing. For more information on the ePrivacy Regulation and how this will impact advertising, please see [here](#).

Misleading and Comparative Advertising Directive

As part of its Smart Regulation policy, the European Commission is running a Regulatory Fitness and Performance Programme, aiming to simplify law, reduce regulatory costs and contribute to a clear, stable and predictable regulatory framework. This process includes a review of the Misleading and Comparative Advertising Directive.

The period of consultation ended on 12 September 2016 and publication of the Commission report is expected in the second quarter of 2017.

Broadband claims

Following a series of research projects into broadband advertising, the ASA and its sister body CAP are moving forward with two separate initiatives. On 31 March 2017, the ASA launched an [investigation](#) into the use of 'fibre' in advertisements for part-fibre broadband services. The ASA's findings are expected in summer 2017. CAP has since published a [public consultation](#) seeking views on different options to 'strengthen the standards around broadband speed claims'. Currently broadband service providers are permitted to use 'up to' claims to advertise their maximum speed, if that speed is achievable by just 10% or more of their customers. The consultation proposes various alternative options to replace this rule, such as 'peak-time median download speed' and a 'range of 24-hour national download speeds available to the 20th to 80th percentile of users'. The consultation closes on 13 July 2017.

Advertising HFSS products:

CAP has announced that from 1 July 2017, advertising of food and drink products high in fat, salt or sugar (HFSS) will be banned in children's non-broadcast media, including print, cinema, online, and social media advertising, targeted at under 16s. This follows Ofcom's research that children aged between 5 and 15 are now viewing online content more than television. For a summary of the new rules see our [update](#). The ASA has also published [guidance](#) on differentiating HFSS product ads from brand TV ads, which fall outside the ban.

In focus: Personal liability

Advertising regulation in the UK has historically been dominated by the self-regulatory/co-regulatory regime operated by the ASA. However, other regulators also have roles to play and have been increasingly active.

Consumer and business protection regulations

The Consumer Protection from Unfair Trading Regulations 2008 (CPRs) and the Business Protection from Misleading Marketing Regulations 2008 apply to advertising communications and generally prohibit misleading actions and omissions. A breach can result in a criminal prosecution, unlimited fine and up to two years' imprisonment. Directors, managers, secretaries or other officers of a company can be liable under the Act if the breach was committed with their consent or connivance. Similar sanctions can be imposed for breaches of other statutory rules governing, for example, gambling, tobacco, pharmaceuticals and e-cigarette advertising.

In 2017, a company director was found guilty of offences under the CPRs after his motor-dealer company provided misleading information to consumers. The company falsely advertised the service history and mileage on two cars and the director was fined £400 and ordered to pay a £30 victim surcharge, £4,750 in compensation and £3,000 in costs, by virtue of his consent, connivance or neglect. The breach came to the attention of Trading Standards via the Citizens' Advice Consumer Helpline.

If a consumer or competitor complains to the ASA about a particular advertisement via their self-regulatory system, the ASA will contact the advertiser directly if it considers the advertisement complained of has broken advertising rules. Directors and employees of advertisers would not normally be personally investigated or named by the ASA.

Dates for the diary

27 June 2017	Section 96 of the Digital Economy Act 2017 in force, requiring the ICO to prepare a 'Direct Marketing Code'.
Q2 2017	CAP to provide an update in relation to the use of 'fibre' in broadband ads.
Q2-Q4 2017	Draft ePrivacy Regulation continues through the legislative process, including consideration by the European Parliament.
Q2 2017	European Commission's 'Fitness Check' of the Misleading and Comparative Advertising Directive and the Unfair Commercial Practices Directive expected to be completed.
1 July 2017	New CAP rules come into force, banning the advertising of HFSS food and drink products in children's non-broadcast media.
13 July 2017	CAP consultation on broadband speed claims closes.
25 May 2018	GDPR becomes directly effective across all EU Members States. ePrivacy Regulation also expected to come into force.

Anti-Bribery, Corruption and Financial Crime



Tom Ellis

Partner

T: +44 20 7105 7418

tom.ellis@osborneclarke.com



Jeremy Summers

Partner

T: +44 20 7105 7394

jeremy.summers@osborneclarke.com

Current issues

Increased international co-operation

The exchange of information, on both a formal and informal basis, between international enforcement agencies continues to grow. This increases the likelihood that the conduct of business executives undertaken overseas will come to the attention of UK authorities and so potentially lead to prosecution here.

Increased whistleblower reports

Similarly, the growing prevalence of whistleblower reports, particularly in the US where they are financially incentivised, provides yet further intelligence and evidence for authorities, which is now more likely to lead to enforcement action being taken than ever before. The Rolls-Royce investigation started with an online whistleblower.

Increased sentences

The most recent guidelines issued by the Sentencing Council in 2014, for 'Fraud, Bribery and Money Laundering Offences', point to the likelihood of more severe sentences being imposed on those convicted of economic crime committed in the course of their work.

Unexplained Wealth Orders (UWO)

The **Criminal Finances Act 2017** brings into force UWOs, allowing the SFO, HMRC and other agencies to apply to the High Court for an order forcing the owner of an asset, valued at over £100,000, to explain how they obtained the funds to acquire it. If the owner cannot demonstrate that the asset was acquired with legal funds, the asset can be seized.

Failure to prevent tax evasion

The Criminal Finances Act 2017 also introduced the new corporate offence of **failing to prevent tax evasion**. The commencement date of the offence is uncertain but it could be as early as September or October 2017. Companies will need to consider what steps they should take to prevent tax evasion, potentially following a methodology familiar to many from the development of adequate procedures to prevent bribery.

Developing SFO pre-requisites to offering a Deferred Prosecution Agreement (DPA):

The SFO's early, but developing, record on DPAs appears to indicate some evolving flexibility. Most notably, the Rolls-Royce DPA was agreed despite the company not self-reporting, something previously understood to be a pre-requisite to a deal. Having the systems in place to understand and react to issues quickly remains key to taking full advantage of the strategic opportunities that may arise, such as self-reporting or otherwise co-operating with the authorities.

In focus: Personal liability

Individual liability can be imposed for bribery or fraud offences under the same key legislation, the Fraud Act and the Bribery Act, that applies to corporates.

It is notable, though, that the most significant economic crime development in 2016 is a point of significant difference between corporate and individual liability. The first deployment of DPAs have involved Standard Bank, Rolls-Royce and so-called 'XYZ Ltd', whose real identity has been concealed pending the possible prosecution of individuals within the company. However, DPAs can only be granted to companies and not to individuals.

Further, as a condition for obtaining a DPA, companies will normally be required to provide evidence with which company personnel may be prosecuted, and increasingly the authorities will be looking, where relevant, at the most senior individuals in the organisation. This may lead to an environment where the company is spared conviction, but at the expense of individuals who may have been following company culture.

Where a potential issue arises, individuals should be considering when they will need to seek independent legal advice on their personal liability, separate from the advice provided by external counsel to the company.

Thought should also be given to the impact on the company when the interests of the individual and the interests of the company begin to diverge. For example, a conflict of interest may develop such that it is no longer appropriate for certain members of senior management to instruct external lawyers (or otherwise be involved in dealing with an issue) on behalf of the company. In this position, both the individual and the company can be better protected if pre-existing procedures are activated to ensure the company continues to have representatives who can act on its behalf. This acutely sensitive issue can also be, to some extent, defused by the engagement of a pre-existing process.

Have there been any notable fines or custodial sentences for individuals?

Tom Hayes was sentenced to 11 years' custody (on appeal) for his role in the LIBOR scandal, and the sentence represents a general upward direction of travel. The years 2017 and 2018 will be watched with interest as a number of high-profile prosecutions proceed, involving senior executives from Alstom, Tesco and XYZ Ltd. They are likely to be informative as to the future approach of the courts. Of perhaps greatest significance will be the decisions taken by the SFO in relation to the Rolls-Royce corruption investigation. This may see the prosecution of the (current or formerly) most senior individuals in the company.

Is this a current area of focus for regulators or prosecuting authorities?

Individuals have always been at risk of prosecution in the event that they act improperly. What has changed, however, is the focus, in both the UK and the US, to look to establish corporate criminal liability and, in doing so, to require the companies concerned to assist the authorities with the prosecution of key individuals. The risk of prosecution now faced by companies, it is hoped, will encourage greater self-reporting, but this in turn will almost certainly lead to greater exposure for individuals.

What can individuals do to protect themselves?

As noted above, individuals cannot obtain a DPA. Individuals, though, may be able to secure full or partial immunity from prosecution or increased mitigation credit under the provisions of the Serious and Organised Crime and Police Act 2005 (SOCPA). Even if a formal SOCPA deal is not possible, early and full co-operation with the authorities will be recognised by the courts, leading to a lesser sentence than would otherwise have been the case.

The decision to engage with the authorities is one that must be taken with great care and caution. The decision will often be highly complex and very finely balanced, and so expert advice should always be sought.

Following applicable company policies and procedures can protect the individual as well as the company. In terms of internal exposure to disciplinary action, employees can help protect themselves by ensuring they can demonstrate full compliance. This may include, for example, keeping copies of receipts indicating that gifts are within permitted thresholds and that, where required, written approval was given. Individuals should also ensure that they document the resolution of any issues that do arise. For example, if a contract omits an anti-bribery and corruption clause, individuals may need to be able to explain that omission (particularly if inclusion is required by company policy and procedure).

Dates for the diary

June 2017	Money Laundering Regulations 2017 come into force.
June/ July 2017	Verdicts and sentencing, if any, in the trial of a number of former senior Alstom executives charged with corruption. This is a significant SFO investigation, which has also resulted in charges against Alstom companies. Two further, separate, Alstom-related trials are due to commence in September 2017 and January 2018.
4 September 2017	Commencement of the trial of three former senior Tesco executives accused of manipulating company accounts. The trial follows a high-profile SFO investigation.
September/ October 2017	Expected commencement date of new failure to prevent tax evasion offence in the Criminal Finances Act 2017.
Late 2017	Possible decision by SFO as to any charges against Rolls-Royce senior employees and officers.
15 January 2018	Commencement of the trial relating to two former directors of XYZ Ltd in relation to corruption. This trial follows a related DPA and may be informative as to the sentencing approach with individuals in the future.

Competition



Simon Neill

Partner

T: +44 20 7105 7028

simon.neill@osborneclarke.com



Marc Shrimpling

Partner

T: +44 11 7917 3490

marc.shrimpling@osborneclarke.com

Current issues

Brexit

The implications for the competition law regime and its enforcement in the UK, including the role the Competition and Markets Authority (CMA) plays, will depend on the outcome of the ongoing negotiations. There are numerous aspects of the EU competition law regime, such as state aid and the safe harbour for vertical agreements, which businesses may be urging the UK Government to retain in force or mirror in the UK post-Brexit.

Geo-blocking

The European institutions continue to debate a ban on geo-blocking – preventing use of a website or the sale of goods to customers based on their geographical location. MEPs voted on a geo-blocking report in April 2017, with the outcome yet to be announced. It is reported that the Commission wanted the Council and Parliament to agree by the end of June. Now that the rules on portability of online content have been agreed, attention is likely to shift to the geo-blocking rules.

Digital comparison tools market study

In March 2017, the CMA announced the second phase in its market study into digital comparison tools (DCTs), such as price comparison websites. Although finding that DCTs enable consumers to compare products/services, make informed choices and save money, concerns were raised around transparency of information, how effectively the DCTs compete, and how DCTs are regulated.

Collective redress

In 2013, alongside its then-draft Damages Directive, the European Commission adopted its recommendation for EU Member States on common principles for injunctive and compensatory collective redress for infringements of EU law. The Commission recommended that Member States implement the principles into their national collective redress systems. The Commission will assess the implementation by 26 July 2017 and consider whether further strengthening measures are required.

21st Century Fox/Sky plc

Following merger control clearance by the European Commission, the UK's Secretary of State for Culture, Media and Sport issued a European Intervention Notice in March 2017, citing grounds of media plurality and commitment to broadcasting standards. Ofcom and the CMA delivered reports on public interests and jurisdictional issues respectively on 20 June 2017.

Energy price cap

In its manifesto, the Conservatives stated that they will review the cost of energy with the ambition that the UK have the cheapest energy costs in Europe. The manifesto stated that they would introduce a safeguard tariff cap to extend the price cap to customers on poor-value tariffs. In light of the Election results, it remains to be seen whether this is something that the Conservatives will look to impose. In any event, there could be scope for energy companies to challenge a regulated price cap if its effect would be to dampen competition or if it is intended to apply only to certain companies' tariffs.

In focus: Personal liability

While liability for infringement of competition law typically rests with the corporate business, in the UK individuals can also be held liable.

Criminal cartel offence

The Enterprise Act allows for criminal prosecution against individuals who have made or implemented, or cause to be made or implemented, arrangements whereby two undertakings engage in prohibited cartel activity. That activity could take the form of price fixing, limitation of production or supply, customer or market sharing, and/or bid rigging.

This criminal cartel offence captures individuals, regardless of their level of seniority within a business, who have played a key part in cartel activity.

Individuals who are found guilty of the criminal cartel offence are liable, on conviction, to imprisonment for a maximum term of five years and/or an unlimited fine.

Previously, for an individual to be guilty of this offence, they needed to be proven to have acted 'dishonestly'. This made it difficult for the competition authorities to bring prosecutions successfully. Since April 2014, however, there is no longer a requirement for the individuals involved to have acted 'dishonestly'. We would, therefore, expect to see more prosecutions under this offence in the future, and the CMA's intelligence and investigation teams are believed to be currently looking into a number of suspected cartels.

Competition disqualification orders

The CMA can apply to the court for a competition disqualification order, under the Company Directors Disqualification Act, in respect of an individual director where:

- the company, of which the individual is a director, commits an infringement of competition law, whether unlawful anti-competitive agreements or an abuse of dominance; and
- the individual's conduct as a director makes them unfit to be concerned in the management of a company.

Where an order is made, the individual will be disqualified from acting as director for up to 15 years.

The CMA secured its first competition disqualification order in December 2016, disqualifying the managing director of Trod Limited for a period of five years. The CMA had found that Trod had agreed with a competitor not to undercut each other's prices for posters and frames sold on Amazon UK.

Enforcement against individuals set to increase

Competition law enforcement, including individual prosecution, remains at the forefront of the CMA's mind. The CMA's latest annual plan for 2017/18 confirms that it is looking to ramp up enforcement in this area and increase the number of investigations each year.

The focus on enforcement highlights the need for individuals to understand what conduct is or is not permissible. Individuals should pay close attention to their organisation's competition compliance policy to understand what may constitute an infringement of competition law. As the defence to the criminal cartel offence illustrates, obtaining legal advice when you are unclear about specific conduct can not only be a way of ensuring that you are not infringing competition law but may also act as a defence in future.

Dates for the diary

Summer 2017	European Commission decision expected in relation to the legality of absolute territorial restrictions in agreements between TV broadcasters and film studios.
Summer 2017	European Commission decision expected in relation to allegations that Google is abusing its dominant position in the CCA markets for internet search services.
13 August 2017	CMA Phase 2 decision due on merger of two NHS Foundation Trusts in Manchester, which could have a significant impact on future consolidation in the UK healthcare sector.
28 September 2017	CMA's final report on digital comparison tools market study expected.
Autumn 2017	EU General Court may deliver judgment on Commission's decision to prohibit the proposed acquisition of Telefónica UK by Hutchison 3G UK.

Consumer Protection



Tom Harding

Associate Director

T: +44 117 917 3060

tom.harding@osborneclarke.com

Current issues

The Digital Single Market

The European Commission's Digital Single Market (DSM) strategy is aimed at providing better access for consumers and businesses to digital goods and services across Europe, including through the harmonisation of consumers' rights across the EU for online purchases of goods and digital content, preventing website geo-blocking and allowing 'portability' of digital content services.

The DSM is a wide-ranging and ambitious strategy, and many of its legislative proposals have to be finalised and implemented, but we expect to see some of them take effect in 2017.

Geo-blocking regulation

In April 2017 the European Parliament **voted** on a consumer-friendly draft Regulation prohibiting outright geo-blocking or auto-redirection without adequate information, and preventing online sellers from discriminating against consumers within the EU based on their nationality and location. Negotiation will now take place between the Parliament, Council and Commission to agree final law, anticipated for early summer 2017.

Portability

In February 2017, the European Parliament, Council and Commission reached agreement on the **proposed portability regulation** to allow consumers to access their online subscriptions (such as Netflix, Amazon Prime and Spotify) in any Member State while temporarily outside their Member State of residence. The Parliament and Council must now formally approve the new rules. For information on how to prepare for the new law, please see [here](#).

eCommerce investigations

In line with the DSM strategy and to break down regulatory barriers that hinder cross-border eCommerce, in February 2017 the European Commission launched three separate **investigations**. These investigations are looking into whether online sales practices breach EU antitrust rules by preventing consumers purchasing cross-border electronics, video games and hotel accommodation at competitive prices. The investigations also focus on price restrictions, location discrimination and geo-blocking. The Commission has also now **published** its final report following its eCommerce sector inquiry.

Brexit

The vast majority of consumer protection law in the UK derives from EU law, but is long-standing, and has been implemented into national law. As a result, while following Brexit the UK would be free to amend existing consumer law (much of which is consolidated into the Consumer Right Act 2015), this seems unlikely. That said, much of the proposed legislation under the DSM is unlikely to have been implemented by the time of Brexit, so the UK will have to decide whether it implements equivalent legislation post-Brexit. Moreover, the UK is unlikely to have much influence on the DSM legislation going forward as a result of the UK now having triggered Article 50, which may influence the UK's decision as to whether to adopt equivalent DSM legislation. See [here](#) for more on how Brexit might affect consumer protection.

ePrivacy Regulation

On 10 January 2017, the European Commission published its proposal for a Regulation on Privacy and Electronic Communications, which will be directly applicable across the EU. The ePrivacy Regulation looks to introduce significant reforms, including amending current direct marketing rules. An important change is that these rules will not only apply to automated calls, email and SMS, but also to communications sent via instant messaging services and in-app notifications.

European Commission Fitness Check

The European Commission is currently reviewing a number of consumer protection Directives, including Unfair Commercial Practices Directive, Sales and Guarantees Directive and Unfair Contract Terms Directive, as part of its Regulatory Fitness and Performance Programme (REFIT). The aim of REFIT is to simplify law, reduce regulatory costs and contribute to a clear, stable and predictable regulatory framework. The consultation period has ended and publication of the Commission report is expected in the second quarter of 2017.

The Commission is also evaluating the Product Liability Directive following its public consultation, which closed on 26 April 2017, to review whether the Directive is fit for purpose in light of technological developments such as the Internet of Things.

Digital Economy Act 2017

The Digital Economy Act received Royal Assent on 27 April 2017. The Act intends to (among other things) improve broadband connectivity, so that consumers have better access to fast broadband, no matter where they are based, and to provide better support for consumers. The Act also intends to provide important protections from spam email and nuisance calls, and protection for children from online pornography, through civil penalties and ISP-level blocking.

Consultation on terms and conditions in consumer contracts

Between 1 March and 25 April 2016, the UK Government ran a consultation on making consumer-facing terms and conditions more accessible. The Department of Business, Energy and Industrial Strategy also ran a consultation in relation to its proposal to introduce civil fining powers for breaches of consumer protection legislation, which the CMA responded to with support. We are still awaiting feedback from both consultations.

In focus: Personal liability

There are two public bodies that enforce much of the UK's consumer law: the Competition and Markets Authority and Trading Standards. Private individuals can also bring claims through the courts to enforce certain consumer protection laws.

Much of consumer protection law focuses liability on the concept of a 'trader', where personal liability rarely exists. There are exceptions, though. Under the Consumer Protection from Unfair Trading Regulations 2008, for example, directors, senior managers and any individuals purporting to act in that capacity can be liable for unfair commercial practices, misleading actions, misleading omissions and aggressive selling techniques. A breach of those Regulations can result in criminal prosecutions, unlimited fines, or a fine and up to two years' imprisonment.

While these sanctions that can be imposed on individuals are rare, they do happen. Recent examples include the following:

- In 2016, a £3,000 fine was imposed on a director of two roofing and windows firms. His companies were also fined £1,000 and £3,000 respectively. The director and the companies were charged with engaging in unfair commercial practices, having stated in their standard consumer contracts that consumers had just seven days to cancel rather than 14, and for misleading customers. The director and companies had ignored previous warnings from Trading Standards, which had included sending the director a template contract to use.
- In 2017, a director of a motor-dealing company was found guilty of providing misleading information to consumers. He was fined £400 for the offences but also ordered to pay £30 as a victim surcharge, £4,750 in damages, split between the two consumers affected, and £3,000 in costs.

Dates for the diary

Q2 2017	Planned completion of the European Commission's REFIT programme.
H1 2017	Finalised European Directive relating to digital content expected.
Q3 2017	Finalised European Regulation relating to geo-blocking expected.
25 May 2018	ePrivacy Regulation expected to come into force.

Cyber Security



Charlie Wedin

Partner

T: +44 117 917 4290

charlie.wedin@osborneclarke.com

Current issues

National Cyber Security Centre (NCSC)

In February 2017, the NCSC was launched to co-ordinate the UK Government's response to cyber threats. Part of GCHQ, the NCSC provides support to infrastructure-critical businesses in the event of cyber incidents, as well as working with experts in a range of organisations to improve cyber resilience. The NCSC will also provide best practice guidance to businesses, based on its research and experience. In its first three months in existence it assisted on 188 serious attacks.

NIS Directive

The EU Network and Information Security Directive requires certain providers of 'critical infrastructure' to take prescribed measures to prevent and minimise the effect of cyber breaches, and to notify the relevant authority of any breaches that take place. The UK Government has indicated that it will implement the Directive on time, regardless of Brexit, although no details of what the measures or who the relevant authority will be have yet been published. A public consultation is expected shortly, but no date has been announced. The sectors covered by the Directive are Energy, Water, Banking, Financial Markets Infrastructure, Transport, Healthcare and Digital Infrastructure. The Directive will also apply to providers of certain digital services, such as online marketplaces, search engines and cloud computing providers.

National governments have until May 2018 (the date that the EU General Data Protection Regulation [GDPR] also comes into force) to set out the minimum standards that the providers of "critical infrastructure" need to comply with, along with sanctions for breach. Those providers must then be identified by November 2018.

Vulnerabilities of connected devices

Although manufacturers are becoming more alert to the security risks posed by unprotected 'connected devices', the Internet of Things (IoT) raises a number of security issues, particularly where users have no ability to update software or incorporate protection into existing products. Security vulnerabilities create dangers to the users of those devices or permit IoT devices to be hijacked and used to mount large distributed denial-of-service attacks.

Ransomware

As the recent **NHS attacks** have demonstrated, 'ransomware' attacks, which involve locking down a computer or wider system then demanding a payment to restore access, are a growing threat for UK businesses. A recent survey commissioned by the Department of Culture, Media and Sport found that almost a fifth of companies had been the victims of such attacks. As with many cyber threats, ransomware often targets individual employees as the 'weak link' in an organisation's cyber security system. It is no longer necessary for criminals to have the IT skills to carry out such attacks themselves, as 'off-the-shelf' ransomware can be readily obtained on the dark web.

Risk mitigation

Despite widely publicised risks and attacks, only 52% of 1,500 firms surveyed in a Government-backed report have implemented the five basic controls that the Government-endorsed Cyber Essentials scheme recommends to prevent 80% of cyber attacks. Even companies with such measures in place can fall victim to a major breach, of course, particularly as a result of the exploitation of its employees, whether maliciously or unwittingly. It is vital for companies to ensure they have a dedicated and stress-tested cyber incident response plan. Along with technical measures such as locating and isolating attack vectors and protecting high-value IP, the plan will need to provide for early-stage investigation, notification (taking into account future obligations under the GDPR and NIS Directive), PR management and any HR issues.

Cyber insurance

Specific cyber security insurance is becoming more common in the UK. The nature and extent of this insurance can vary widely, but with premiums in some other areas reducing, many businesses are now considering the addition of cyber security insurance. This is particularly important as industry surveys typically reveal a gap between the levels of cover that businesses think they have under non-specialist policies and the actual levels of cover under those policies for cyber breaches.

In focus: Personal liability

It is unlikely that individuals within a company that experiences a security incident will face any personal prosecution in relation to that data breach or cyber incident, unless they themselves caused the incident. However, given the reputational impact of these incidents, they are generally board-level issues and senior executives and board members can find themselves under intense pressure if they are responsible for failings that led to breaches or fail to respond appropriately. It is, therefore, vital that senior executives and board members understand their responsibilities and practise responding to data breach scenarios.

More often, individuals are the subject of offensive action by the company suffering the security incident. Where the perpetrator of an attack is unconnected to the company, this will mean co-operating with law enforcement authorities. This can reduce the level of a control that the company has over issues such as information flow, which may need to be borne in mind when considering notification to customers and supply-chain partners, and to reputation management.

When breaches involve employees or ex-employees, companies may need to consider taking action themselves against those individuals, such as obtaining injunctions to search properties and/or recover data or intellectual property.

Where such action appears necessary, it is important to act quickly, before vital information or evidence can be released or deleted. The ability to react quickly following a breach will be a vital part of a well thought-out and comprehensive risk-mitigation strategy as discussed above.

Dates for the diary

9 May 2018	Deadline for the NIS Directive to be implemented into national law.
-------------------	---

25 May 2018	GDPR comes into force.
--------------------	------------------------

Data Protection and Privacy



Mark Taylor

Partner

T: +44 20 7105 7640

mark.taylor@osborneclarke.com

Current Issues

General Data Protection Regulation (GDPR)

The GDPR will take effect across the EU from 25 May 2018. The GDPR introduces some significant changes that have the potential to have a profound impact on many organisations that collect and use information about individuals.

Over the next few weeks and months, we are expecting individual EU Member States to implement the requirements of the GDPR into national law, particularly in areas in which Member States are able to derogate from the requirements of the GDPR (such as in relation to the use of special categories of personal data and transfers outside the EEA). We await the outcome of the UK Government's **consultation** on the potential derogations to be adopted in the UK, which closed on 10 May 2017. We are also expecting further guidance to be issued by the Information Commissioners Office (ICO) and the Article 29 Working Party (WP29).

The WP29s Action Plan for 2017, published on 3 January 2017, includes the intention to issue guidance on: administrative fines; certification; profiling; consent; transparency; notification of personal data breaches and tools for legitimising transfers outside the EEA.

In July 2017, the ICO expects to release the final version of its draft **guidance on consent** under the GDPR. It also intends to publish guidance on contracts and liability, and is considering the implications of the GDPR for profiling and the processing of personal data relating to children.

You can find out more about the GDPR on Osborne Clarkes dedicated **GDPR Feature** page.

Brexit

In February 2017, the UK Government confirmed that the UK would maintain a GDPR-equivalent regime post Brexit. The UK will need to convince the European Commission that the broad scope of the UK Governments surveillance powers in the Investigatory Powers Act 2016 do not undermine the level of protection afforded to personal data in the UK,

if the UK wants to be deemed adequate for the purposes of facilitating EU-UK data transfers.

Data transfers outside the EEA

We await the Irish High Courts judgment in the case of Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems.

The Data Protection Commissioner (DPC) has asked the Irish High Court to make a Preliminary Reference to the Court of Justice of the European Union (CJEU) as to the validity of the standard contractual clauses for legitimising transfers of personal data outside the EEA (otherwise known as the Model Clauses).

The intended referral to the CJEU does not mean that the Model Clauses are now invalid. It is likely to take some time for the CJEU to pass judgment on the Model Clauses so until we hear anything different (from the CJEU or from regulators) the Model Clauses should continue to be used.

e-Privacy Regulation

On 10 January 2017, the European Commission published its **proposal** for a Regulation on Privacy and Electronic Communications (e-Privacy Regulation) to replace the existing e-Privacy Directive (implemented in the UK by the Privacy and Electronic Communications Regulations 2003). It aims to reinforce trust and security in digital services in the EU, by ensuring a high level of protection for privacy and confidentiality in the electronic communications sector, as well as seeking to ensure the free flow of movement of personal data and of electronic communications equipment and services in the EU.

The draft e-Privacy Regulation introduces significant reforms (summarised **here**), including in relation to the (much broader) scope and territorial application of the rules, the processing of electronic communications data, and the so-called cookies rules (which, of course, cover a much wider range of technologies and activities than simply posting and accessing cookies).

Both the WP29 and the European Data Protection Supervisor have published their opinions on the draft e-Privacy Regulation. The final text of the e-Privacy Regulation is expected later this year. The original ambition of the European Commission was for the e-Privacy Regulation to come into effect on 25 May 2018 – the same date as the GDPR, although that does seem a little optimistic.

In focus: Personal Liability

Data Protection Act 1998 (DPA)

Generally, directors, officers and employees of companies have no personal liability for breaches of the DPA that are committed by their companies as data controllers. However, this does not remove the ability for individuals to commit specific offences personally.

For example, under section 55 of the DPA, it is a criminal offence to knowingly or recklessly, without the consent of the controller:

- obtain or disclose personal data (or the information contained in personal data); or
- procure the disclosure to another person of the information contained in personal data.

There are plenty of (very recent) examples of the ICO prosecuting individuals under section 55 of the DPA, although fines tend to be low. A typical, recent, example from April 2017 involved a former clerical officer being fined £650 and ordered to pay costs of £654.75 and a victim surcharge of £65 after accessing the sensitive medical records of two estranged family members without the consent of the data controller. The data controller was the individuals former employer.

Privacy and Electronic Communications Regulations 2003 – Direct marketing

In **response** to the controversy over directors lack of accountability, the UK Government announced its intention to give additional powers to the ICO to fine company directors up to £500,000 for certain breaches of the PECR. This is in a move to tackle the trend of using liquidation as a means for companies to escape paying fines.

The plans were expected to be implemented from spring 2017, but have since been delayed.

GDPR

The GDPR retains the position that directors, officers and employees of companies have no personal liability for breaches of the GDPR. Under the GDPR, there is no equivalent provision to section 55 of the DPA.

However, sanctions, powers and the general conditions for imposing administrative fines are all areas in which Member

States are able to derogate from the GDPR. In particular, Recital 149 of the GDPR allows Member States to lay down the rules on criminal penalties for infringements of the GDPR.

The outcome of the UK Government's consultation on the potential derogations to be adopted in the UK (referred to above) should shed some further light on this issue. We would expect, at the very least, that the UK will seek to include an equivalent criminal offence to that which is contained in section 55 of the existing DPA.

Dates for the diary

Spring 2017	New ICO enforcement power £500,000 fine against company directors under PECR.
Summer 2017	ICO guidance on consent – final version expected to be published following the consultation, which closed in March.
Summer 2017	Summary of responses expected from the ICOs feedback request in relation to profiling under the GDPR, which closed in April.
Summer 2017	Irish High Court judgment in the case of Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems expected (in relation to the Model Clauses).
Throughout 2017	Further guidance from the WP29 expected on various aspects of the GDPR (including administrative fines, certification, profiling, consent, transparency, notification of personal data breaches and tools for legitimising transfers outside the EEA).
Summer/ Autumn 2017	Final text of the e-Privacy Regulation expected to be approved.
25 May 2018	The e-Privacy Regulation (once finalised) is anticipated to come into effect.
25 May 2018	The GDPR comes into effect.

Dual-Use Goods and Export Control



Emily Jones

Partner

T: +1 650 714 6386
emily.jones@osborneclarke.com



Jon Round

Senior Associate

T: +44 11 7917 3400
jon.round@osborneclarke.com

Current issues

New monetary penalties for breaches of financial sanctions

The Office of Financial Sanctions Implementation (OFSI) was established on 1 April 2016. Exactly a year later, Part 8 of the Policing and Crime Act 2017 came into force, which creates powers for HM Treasury to impose monetary penalties for breaches of financial sanctions. OFSI will apply these powers.

Previously, breaches of sanctions could only be punished by criminal proceedings, which were subject to the requisite criminal standard of proof. However, OFSI now has the power to impose financial sanctions, for which it only needs to satisfy the lower civil standard of proof. OFSI has published [general guidance](#) and [monetary penalties guidance on how it will use these powers](#).

Companies should review their sanctions compliance policies and procedures to ensure they stand up to scrutiny in light of the new powers now available to the OFSI. For more information see [here](#).

Modernisation of European dual-use export control regime

The European Commission has for several years been involved in an extensive consultation about the European dual-use export control system. On 28 September 2016, the Commission published a [proposal](#) to amend the legislation underpinning the current European dual-use export control regime, the EU Dual-Use Regulation. The proposed changes aim to harmonise, simplify and introduce a new 'human security' dimension to the existing European dual-use export control regime. You can find our overview of the changes [here](#).

The proposals are currently being decided upon by the European Council and the European Parliament. The European Council's Working Party on Dual-Use Goods is meeting on a monthly basis to discuss the changes – you can follow progress on those discussions [here](#). The European Parliament has confirmed that it is also preparing a position on the proposal.

Brexit: Export controls on dual-use items

The UK has developed a robust dual-use export control regime, which is independent but inextricably tied to the EU's export control framework. The UK is also, independent of its membership of the EU, a member of a number of international conventions on human rights or non-proliferation (for example, the Wassenaar Arrangement). For these reasons, in the short term, Brexit is unlikely to raise any barriers to the flow of dual-use goods between the UK and other EU Member States and the types of controlled items and technology are expected to remain broadly similar.

In the medium/longer term, while any major departures from existing dual-use practices remain highly unlikely, at least for as long as the UK's strategic foreign policy and defensive interests remain broadly similar to those of EU Member States, some level of divergence could creep in over time. For example, if the amendments to the EU Dual Use Regulation summarised above are not implemented before the UK formally leaves the EU, they will not apply automatically to the UK. These distinctions could be perpetuated by the UK's shifting foreign policy interests, such as its desire to use the UK defence industry to strengthen the UK economy in light of Brexit and its developing relationship with the US administration.

In focus: Personal liability

Directors, officers and employees of businesses involved in exporting dual-use items from the UK can incur extensive levels of personal liability under the UK dual-use export control regime. For example, under the Customs and Excise Management Act 1979 (CEMA), exporting dual-use goods with "intent to evade" a restriction or prohibition is chargeable with a fine or a criminal sentence of up to ten years. Related, albeit less serious offences may be brought against individuals in their personal capacity on a "strict liability" basis, meaning that a person could incur civil liability even if they were unaware of the relevant export control.

CEMA does not distinguish between individuals on grounds of role or seniority within a business. As a result, any individual operating for, or on behalf of, a business can be held personally liable, provided that they are “concerned” in the export (or attempted export) of items in breach of relevant restrictions. This has potentially wide-reaching implications for employees at all levels of a business, although in practice the UK authorities focus their attention on senior management.

Despite these wide-ranging enforcement tools, the number of published personal prosecutions for export breaches in the UK remains relatively low, particularly when compared to equivalent figures in the US. However, individuals still remain key targets of aggressive and robust enforcement from the UK authorities: the Export Control Organisation; HMRC; the UK Border Force; and the Criminal Prosecution Service. The ECO has been keen to stress that there have been three high-profile prosecutions for UK export control offences in as many years. For example, in 2014 the Managing Director of Delta Pacific Manufacturing Limited was jailed for two and a half years, and fined £68,000, for exporting specialised alloy valves to Iran in breach of UK dual-use export control laws – the alloy valves were routed through Hong Kong and Azerbaijan in order to conceal their final destination and avoid UK export controls, in breach of section 68 (2) CEMA.

Managing regulatory risk to individuals

The very nature of ‘strict liability’ offences means that such prosecutions will not be defended except in very limited circumstances. ‘Intent to evade’ cases, by contrast, remain highly fact-specific and typically turn on the subjective question of what the defendant, in fact, knew. Nevertheless, businesses can minimise the risks of breaching the dual-use export control regime, and the related personal liability of those acting on its behalf, through robust and effective internal export control compliance policies and procedures. The ECO would expect these policies to include:

- a firm commitment to export control compliance from a senior stakeholder;
- clear export control compliance procedures (such as checklists to ensure that the correct licences are obtained); and
- a mechanism for delivering comprehensive training and guidance to relevant staff. For example, businesses should develop awareness among employees about identifying suspicious orders/end-use considerations at an early stage in the sales process.

Effective export control breach management procedures, including the early adoption of the right tactical strategy following a breach, are also crucial for minimising personal liability. This is particularly true in light of the increasing use by HMRC of compound penalties: a fine by which HMRC can offer businesses or individuals the chance to settle cases that would otherwise justify being referred to the CPS (generally in a bid to avoid an expensive and protracted [taxpayer funded] criminal investigation).

Dates for the diary

-
- June 2017** The UK House of Lords EU External Affairs Sub-Committee is undertaking an inquiry into UK sanctions policy after Brexit. The inquiry heard evidence during June.
-
- 23 June 2017** The Foreign & Commonwealth Office has published a white paper consulting on the legal powers it will need to be able to continue imposing and implementing sanctions once the UK leaves the EU. Its focus is on the legal powers necessary to operate UK sanctions and not on the shape of UK sanctions policy in the future or other policy issues. The consultation closed on 23 June 2017.
-
- July 2017** The UK Government will publish the UK Strategic Export Controls Annual Report 2016 in July 2017. This report will cover the UK’s export control policy and practice during the period January 2016 to December 2016.
-
- Mid 2017** High Court expected to hand down its judgment following its judicial review into the legality of the UK Government’s continued approval of new licences for the sale of arms to Saudi Arabia (see our commentary on that review [here](#)). If the Government’s position is not supported, this could have major implications for the UK’s legal and regulatory export control framework, so we expect swift action from the Government in the event of an unfavourable decision.
-
- Throughout 2017** EU looks set to continue expanding its sanctions on North Korea in relation to its apparent violations of UN resolutions and the threat it poses to international peace and security.
-

Employment and Contingent Workforce



Julian Hemming

Partner

T: +44 117 917 3582

julian.hemming@osborneclarke.com



Kevin Barrow

Partner

T: +44 20 7105 7030

kevin.barrow@osborneclarke.com

Current issues

Gender pay

The new gender pay reporting requirements came into force in April 2017. They require employers with 250 or more employees to publish a report containing prescribed gender pay gap data. The Government has published final regulations that provide a long-stop date of 4 April 2018 for employers to make their first gender pay report. An employer must report on a 'gender pay snapshot' taken on 5 April 2017.

Details of ordinary pay and bonus pay made in the 12 months leading up to 5 April 2017 will, therefore, form part of an employer's gender pay calculations. The Government has also consulted on gender pay reporting in the public sector and it is likely that the private and public sector requirements will be aligned.

Gig economy

In November 2016, Matthew Taylor was asked by the Government to conduct a review into how the gig economy is affecting workers' rights. He was expected to announce the results of his review in June. A number of claims regarding worker status are also progressing in the courts off the back of an employment tribunal decision to award Uber drivers worker status rather than self-employed. This meant that they were entitled to basic worker rights such as the national minimum wage and paid annual leave.

Holiday pay

The Court of Appeal decided in the Lock holiday pay case that results-based commission must be included in statutory holiday pay calculations. Employers must also bear in mind that regular overtime forming part of normal remuneration may also now be required to be included in statutory holiday pay. Failure to include these payments in future holiday pay entitlements could result in claims under the Working Time Regulations or the deduction from wages provisions in the Employment Rights Act 1996. The Supreme Court has refused an appeal to the Court of Appeal decision in Lock and we are currently awaiting the case returning to the

Employment Tribunal, where it is hoped more guidance will be provided on how results-based commission should be dealt with in holiday pay calculations.

Apprenticeship levy

Funding of apprenticeships changed from April 2017. Employers operating in the UK have to pay a levy, calculated at 0.5% of an employer's pay bill, although a "levy allowance" of £15,000 per year will mean that in practice only employers with an employee pay bill of over £3m will be caught. An employer's levy payments will be paid into the Government's new Digital Apprenticeship Service (DAS), from which they will be able to access the funds (plus a Government top-up) to fund approved apprenticeship training. Employers should start planning how they will use this levy as it is paid into the DAS on a 'use it or lose it' basis, i.e. if an employer does not use its funds within its DAS account within a specific period, they will be made available to another employer.

Taxation of termination payments

It is anticipated that changes to the taxation of termination payments will be introduced from April 2018. The main changes involve: removing the distinction between contractual and non-contractual PILON clauses, to treat both as fully taxable earnings (subject to income tax, employer and employee NICs); and levying employer NICs on other termination payments above the £30,000 limit.

Personal Service Company (PSC) engagement in the public sector

Rather than being able simply to accept the assurances of PSCs engaged by the public sector about tax and IR35, as had been the case, public sector engagers now face a new 'duty' to ensure all PSCs they use pay enough tax. Liability to pay the correct employment taxes has moved from the worker's own company to the public sector body or agency/ third party paying the company.

Employment law reform

A number of employment law reforms are in motion and may well come into force during 2017/2018, including:

- corporate governance reforms, focusing on executive pay, directors' duties and the composition of boardrooms, including worker representation and gender balance in executive positions; and
- we are awaiting the outcome of a Government call for evidence on post-termination restrictions in employment contracts.

In focus: Personal liability

Discrimination, harassment and victimisation

While from an employment law perspective, litigation tends to be brought against employers, it is worth remembering that employees can be held personally liable for acts of discrimination, harassment or victimisation carried out during their employment and, as such, may be joined as individual named respondents in Employment Tribunal proceedings for such claims. An individually named employee will not escape liability even if their employer has successfully defended the litigation against them on the basis that as an employer they had taken all reasonable steps to prevent the discrimination or harassment occurring.

It does not matter that an employee did not know he or she was breaking the law. The only defence to this is if their employer has told them that doing the act was not a contravention of any law. Employers could be faced with a fine of up to £5,000 for making a false statement in order to induce an employee to carry out unlawful conduct.

Negligence and breach of statutory duties

Employees also risk claims of professional negligence being made against them personally (and consequently many employers take out professional indemnity insurance to cover their employees against the risk of such claims) and may also be personally liable under other statutory provisions such as health and safety and criminal laws.

It is also worth noting that directors and senior employees may be required to 'sign off' on certain reports that an employer is required to provide under statute. Recent examples of this include the requirement to provide a statement on modern slavery and the duty on an employer (with 250-plus employees) to report each year on their gender pay gap.

Dates for the diary

Summer 2017	Report coming out of the Taylor Review of Employment Practices in the Modern Economy expected to be published.
During 2017	New tax-free childcare scheme being rolled out.
By the end of 2017	Final report on e-balloting to be laid before Parliament.
2018	Reforms extending shared parental leave to grandparents were previously announced to be introduced in 2018. However, no further information has been forthcoming on this.
April 2018	Potentially changes to the taxation of termination payments may be introduced.

Environment



Matthew Germain

Legal Director

T: +44 117 917 3662

matthew.germain@osborneclarke.com

Current issues

UK Air Quality Plan

On 5 May 2017, the UK Government published its Draft Air Quality Plan, after the High Court rejected its application to extend the deadline for publication of the draft Plan until after the general election. The final Plan must be published by the end of July. The publication of the Plan follows ClientEarth's successful judicial review challenge in November 2016 against the Government's failure to tackle illegal air pollution. The High Court subsequently ordered the Government to publish a new UK Air Quality Plan for consultation by 24 April 2017 (to be submitted to the European Commission by 31 July 2017).

The draft Plan proposes the implementation of Clean Air Zones by local authorities as the most effective way of reducing nitrogen dioxide emissions. Although the proposal does not state that charges will be payable to enter or move within a zone, the proposal states that 'where a charging Clean Air Zone would bring forward achievement of statutory NO₂ limit values... local authorities should have the opportunity to identify and implement equally effective non-charging alternatives'. The proposal has been criticised by parties concerned that non-charging zones will not deter the most polluting vehicles compared to charging zones. While the Plan makes clear that air pollution has social costs and threatens economic growth – with estimates that in 2012 poor air quality resulted in costs of up to £2.7 billion through its impact on productivity in the UK – the introduction of the Zones could have a significant impact on businesses that rely on frequent movement into and within the Clean Air Zones.

Brexit – uncertainty over post-Brexit environmental laws

The Government's Great Repeal Bill White Paper states that it will ensure that 'the whole body of existing EU environmental law continues to have effect in UK law' following Brexit. While this undertaking has helped clarify the Government's initial intentions on environmental policy post-Brexit, there will be areas of uncertainty, and some

concerns have been raised about the use of secondary legislation to address these areas. Secondary legislation is subject to less Parliamentary scrutiny and there is nothing to rule out the possibility of amending, repealing or reversing existing environmental provisions. Green groups have further criticised the Great Repeal Bill for failing to address the status of European Commission guidance in post-Brexit Britain and especially what mechanism/enforcement agency will replace the Court of Justice of the European Union and the European Commission. Businesses will be waiting for further guidance from the Government on some of these more challenging issues, and where relevant should be looking to engage with the Government to highlight the areas where potential regulatory changes could have a positive economic impact.

The Government has also received criticism from businesses and NGOs over the delay caused by Brexit to the publication of DEFRA's 25 Year Environment Plan, a long-term management strategy for the UK's environment. DEFRA's publication of the Plan's framework last summer was put on hold due to the fact that the original timings of the framework 'did not take into account [Britain's] decision to leave the EU'. No new timescale for a post-Brexit Plan has been released.

Contamination land – register of brownfield land to be published

On 16 April 2017, the Town and Country Planning (Brownfield Land Register) Regulations 2017 came into force. The Regulations impose a duty on local planning authorities (LPAs) in England to prepare, maintain and publish a register of brownfield land that is suitable for development in its area. Each register will refer to: (1) brownfield land suitable for residential development; and (2) brownfield land that the LPA has allocated for residential development. It is the Government's intention that these new measures unlock brownfield sites for thousands of new homes, as developers will be able to identify suitable brownfield sites quickly. It is anticipated that communities

will also be able to highlight local derelict and underused buildings sites that are primed for re-development, with the hope of attracting investment.

Guidance on Minimum Energy Efficiency Standards (MEES) for non-domestic rented buildings

In March 2017, the Government published guidance to clarify some aspects of the Energy Efficiency (Private Rented Property) (England and Wales) Regulations 2015 in relation to non-domestic rented properties. The Regulations introduce minimum energy efficiency standards, which from 1 April 2018 will prohibit the letting of a non-domestic property with an EPC rating below Band E and from 2023 will extend the prohibition to properties already let. The guidance is not legally binding but explains how the Government intends the Regulations to be applied. The guidance also sets out how the Government will deal with relevant exemptions to the prohibition, such as listed buildings, those with no EPC in place, and leases under six months or over 99 years.

Water pollution: record fine for Thames Water Utilities Ltd

On 22 March 2017, Thames Water was fined an unprecedented £20,361,140 for a series of significant pollution incidents on the river Thames between 2012 and 2014. Major environmental damage was caused along 14km of river, resulting in the deaths of birds, fish and invertebrates and which also contributed to widespread disruption to local businesses, waterside residents and farmers. Investigations showed the illegal discharge by Thames Water of untreated or poorly treated raw sewerage into the Thames River and its tributaries.

In focus: Personal liability

Despite the Environment Agency being encouraged to use more civil/administrative sanctions (e.g. administrative fines, notices and undertakings), the majority of environmental statutes contain offences that are dealt with under criminal law. As part of that criminal liability these offences commonly contain a potential sanction for individuals; not only as the primary offender as a legal person, but also where it can be demonstrated that an offence of a company was carried out with the consent, connivance or neglect of company officers. These 'parasitic offences' (as they are commonly termed) are mostly used in waste offences (Environmental Protection Act 1990) or breaches of environmental permits (Environmental Permitting Regulations 2016). Few statutes contain a statutory defence and rather it is normally the operational conduct of the defendant company officer that is crucial.

Have there been any notable fines or custodial sentences for individuals?

The majority of large personal liability fines under environmental law have been in relation to waste offences where individuals have intentionally sought to circumvent the law (and avoid landfill tax) through storing or disposing of waste illegally. The largest personal fine in 2016 was £120,000 with five prison sentences.

Is this a current area of focus for regulators or prosecuting authorities?

Certainly in the waste sector where there is a big focus owing to the enormous economic cost of waste crime: a recent report by Eunomia estimated that waste crime costs the UK economy over £600m per year. However, with the new environmental sentencing guideline having a real impact (as seen by the £20m fine for Thames Water this March) in other sectors, notably water, the focus on personal liability is likely to follow other sectors such as construction and other large utilities. Indeed, many commentators were surprised that a personal prosecution did not take place in the Thames Water case.

What can individuals do to protect themselves?

A common-sense approach can help to manage personal liability: if a person becomes aware of something that is or could be a breach of environmental law with serious ramifications, don't ignore or sit on that knowledge. Make sure any incidents are appropriately reported at board level, where decisions can be taken on early engagement with the relevant regulator (usually the Environment Agency).

Dates for the diary

15 June 2017	Government consultation on Draft Air Quality Plan closed.	31 December 2017	Deadline for local planning authorities to publish brownfield land registers.
18 June 2017	Government consultation on penalties for litter offences closed.	End of 2017/ beginning of 2018	DEFRA's "25 Year Plan for the Environment" expected.
25 June 2017	Government consultation on changing the Ultra Low Emission Zone for Central London closed.	1 April 2018	Introduction of prohibition on the letting of non-domestic properties with an EPC rating below Band E under MEES Regulations.
9 July 2017	The Conflict Minerals Regulation comes into force, with due diligence obligations to apply later, from January 2021. Companies within the EU will be under an obligation to ensure that imports of conflict metals and minerals are obtained from responsible sources only.	January 2019	Legislation is expected to come into force that will set binding emission limit values on relevant air pollutants from diesel engines. The proposed legislation follows the Department of Environment and Climate Change's consultation on further reforms to the Capacity Market in March 2016.
31 July 2017	Deadline for publication of the Government's Air Quality Plan.	September 2020	Ultra Low Emission Zone to be introduced for central London.
Summer 2017	A comprehensive update to the European Chemical Agency's guidance on REACH substances is expected to be published.		
Autumn 2017	White Paper on "25 Year Plan for the Environment" expected.		
19 December 2017	Deadline for the implementation of the Medium Combustion Plant Directive 2015.		

Health and Safety



Mary Lawrence

Partner

T: +44 117 917 3512

mary.lawrence@osborneclarke.com

Current issues

Fines soar in first year of sentencing guidelines

Fines for breaches have tripled since the introduction of new sentencing guidelines on 1 February 2015. 19 companies received fines of a million pounds or more in 2016 compared to four in 2015 and none at this level in 2014. Seven-figure fines are no longer limited to cases involving serious injury or death. For more information see [this joint report](#) prepared by IOSH and Osborne Clarke.

HSE Fee for Intervention scheme

The Health and Safety Executive has finally responded to concerns from health and safety duty-holders that Fee for Intervention challenges should not be determined by the HSE itself. The concerns were raised in the initial consultation and its triennial review in 2014, as a result of a judicial review brought by OCS Group. A consultation has been issued, proposing that disputes will be heard by a lawyer and an entirely independent panel. It is understood that the proposal is to introduce a new scheme by 1 September 2017.

Privilege and accident investigation reports

Companies have long carried out full and open investigations into accidents in the belief that their findings would be covered by legal professional privilege and, therefore, protected from disclosure to the regulator (the HSE and/or the police). Companies will now need to be more cautious following a landmark legal professional privilege case brought in May 2017. Mrs Justice Andrews ruled that the commencement of a criminal investigation does not mean that there is 'reasonable contemplation of litigation'. Andrews J also ruled that only documents created with the 'dominant purpose' of conducting a defence to litigation/a prosecution, rather than avoiding the prosecution, or indeed fact-finding, will be protected. The judgment is likely to be appealed but organisations should take great care when drafting witness statements and investigation reports as this case increases the risk that they may end up being disclosable to the regulator.

Mental health moves up the agenda within the HSE and organisations

Health and well-being has historically been an area that is under-enforced by the HSE, but this looks likely to change following the first Stress Summit held by the HSE in March 2017. During the summit, the legal duty on employers to manage the health and well-being of staff was reiterated, and the HSE published a new stress tool. This follows the Prime Minister's commissioning of an initiative to create a new mental health partnership with employers. Organisations are also increasingly interested in strategies to minimise mental health risks, especially given latest figures by bodies such as Mind and Business in the Community that show the substantial losses suffered by businesses due to mental health issues among staff.

In focus: Personal liability

All employees are under a general duty while at work to take reasonable care for the health and safety of themselves and of others who may be affected by their acts or omissions at work, and to co-operate with their employer so far as is necessary to enable it to comply with its own health and safety duties (section 7 Health and Safety at Work, etc. Act 1974).

For a successful prosecution of a director/senior officer, a breach of health and safety law by an organisation must have been 'committed with the consent or connivance of, or to have been attributable to any neglect on the part of any director, manager, secretary or other similar officer of the body corporate'. The test is broad and covers not only where a director/senior officer actively consents or 'turns a blind eye' to the matters that lead to breach, but also where the director/senior officer was unaware but should have made reasonable enquiries of the matters that led to breach.

Individuals can also face prosecution under the common law offence of gross negligence manslaughter, although this will apply only in the most serious cases, where there is evidence that they grossly breached a duty of care that caused or significantly contributed to a death.

Have there been any notable fines or custodial sentences for individuals?

A construction boss was sentenced on 5 May 2017 to twelve months' imprisonment for gross negligence manslaughter following the death of a lawyer crushed by a stack of large window frames that collapsed on her as she walked past a building site in London. The site manager was found guilty and sentenced to six months' imprisonment, suspended for two years.

Is this a current area of focus for regulators or prosecuting authorities?

Yes. In 2015-2016, it was reported that 46 company directors and senior managers were prosecuted under health and safety law, compared to an annual average of 24 in the previous five years. The new sentencing guidelines increase the likelihood of a director going to prison, not only where breaches are intentional but also where there is a flagrant disregard or a 'blind-eye' mentality shown by directors.

What can individuals do to protect themselves?

Directors and senior officers can minimise the risk of prosecution by ensuring that the company does not breach its duties under health and safety law. In practice, this can be effectively done by following HSE guidance documents 'Leading Health and Safety at Work' and 'Managing Health and Safety at Work'. These documents provide advice on how directors and those in senior management positions can implement an effective health and safety system and governance regime to ensure that appropriate procedures are in place to minimise risk and that a robust reporting structure is implemented to alert those at a senior level to any required action.

Evidence to show that this has been properly considered and implemented will be a good defence should an individual director be prosecuted alongside (or instead of) the company. Companies should also check their Directors and Officers insurance to ensure adequate cover for legal expenses in the event of a prosecution against an individual director or senior officer.

Dates for the diary

2 June 2017	HSE consultation on proposals to make the dispute process under the FFI Scheme entirely independent closed.
Summer 2017	HSE expected to issue a discussion document with the intention of simplifying the regulations on hazardous substances, lead, and dangerous substances and explosive atmospheres.
1 September 2017	Likely date for introduction of new HSE disputes process under the FFI scheme.
Late 2017/ early 2018	Publication of the delayed international standard on occupational health and safety management systems (ISO 45001).

Product Regulation



Katie Vickery

Partner

T: +44 20 7105 7250

katie.vickery@osborneclarke.com



Claire Temple

Associate Director

T: +44 20 7105 7034

claire.temple@osborneclarke.com

Current issues

Civil drones (small unmanned aircraft)

The Government's consultation on civil use of drones closed on 15 March 2017. We await the Government's response. The consultation featured a number of regulatory proposals including that anyone who buys a drone has to register it and take a safety test. We anticipate the response will lead to either additional regulation, or a step change in the way existing drone regulation is monitored and enforced.

Driverless cars

The Government has provided an £8.6 million grant to a British consortium to test driverless cars on UK roads in 2019. This is indicative of the Government's desire for the UK to be seen as a frontrunner in this area and backs up what was touted as the motivation for the Vehicle Technology and Aviation Bill (previously the Modern Transport Bill). However, this Bill was not passed before Parliament was dissolved for the general election. It remains to be seen whether the Bill will be reintroduced in the same form, and how quickly this will progress through Parliament. Regulatory change in this area may not take effect until later this year or next.

Predicting the impact of Brexit on CE marking

The practical impact of Brexit on the CE marking product regulation regime currently in place is still unclear. Our prediction is that the UK will either maintain the scheme, as it would still allow UK manufacturers to sell throughout the EU, or adopt a similar but more relaxed regime, which might allow for more innovation but could leave manufacturers that sell in the UK and the EU having to comply with separate regulatory regimes.

Medical devices

The New Medical Devices Regulation and IVD Regulation have now been published. The new EU Medical Devices Regulation came into force on 25 May 2017, marking the start of the three-year transition period for manufacturers selling medical devices into Europe.

The transition period allows manufacturers time to update technical documentation and processes to meet the new requirements. However, they will now find themselves subject to greater scrutiny of technical documentation, clinical evaluation, post-market clinical follow-up, and traceability of devices through the supply chain.

Product Safety and Market Surveillance Package

The long-awaited new package of legislative measures aimed at improving EU consumer product safety and strengthening market surveillance of products is still not yet in force and there is no clear date set for this. From a practical perspective, it would be preferable to have the new legislation in place prior to the Great Repeal Bill, which is expected to convert all EU law as at the date of Brexit into UK law. This would ensure that manufacturers that sell in the UK and EU only have one set of rules to comply with for the foreseeable future.

In focus: Personal liability

Non-compliance with product safety related regulation carries a risk of personal liability for directors, managers and officers. While product regulation encompasses a range of different regulations, the detail of which will differ, most offences require that the company is guilty of an offence, and that the offence was committed with the consent, connivance or neglect of that individual.

Offences are punishable by fines and prison sentences. For more serious offences, fines could be unlimited and prison sentences could be up to 12 months. Directors can also be disqualified.

However, in practice, for non-food consumer products, we tend to see very little in the way of personal liability prosecutions. The focus of the regulators (such as Trading Standards) is typically on securing compliance through active engagement with the company as a whole (as opposed to individual officers).

There have been only a small number of significant prosecutions against companies and even fewer prosecutions against directors.

For example, even where we learn of household names supplying unsafe products, personal liability prosecution often doesn't follow.

–In December 2016, Poundworld was ordered to pay over £190,000 in fines and costs after selling thousands of faulty phone charger kits with forged safety test certificates to UK consumers. Poundworld was criticised by the judge for slow handling of the matter and for failure to have developed a robust testing regime to ensure product safety. Despite this, there were no follow-on prosecutions of directors.

–Similarly, in November 2015, Poundstretcher was ordered to pay £370,000 in fines and costs following the sale of faulty batteries. The batteries were found to be leaking or out of date. Again, the company was criticised for appearing not to have established procedures in place for dealing with the issue, even once they were fully aware of the problem. However, there were still no prosecutions of directors.

Despite this, directors, managers and officers should not ignore the potential for personal liability. The post-Brexit world might require the UK's regulators to be more litigious (more 'stick' than 'carrot') in order to demonstrate to the outside world that they take product safety seriously.

There is a defence of due diligence available if the relevant director, manager or officer can demonstrate they took all reasonable steps and exercised all due diligence to avoid committing the offence. Even though prosecutions are infrequent in this area, it is still important for directors, managers and officers to ensure that they can avail themselves of this defence, if ever required.

Practically, it means:

- having in place robust procedures for the testing of products to ensure full regulatory compliance before products are placed on the market;
- ensuring there is a strong market surveillance process, which can pick up and act swiftly on any reports of product safety incidents; and
- ensuring these processes are well known in the business (particularly by directors, officers and managers), are implemented effectively, and are updated on a regularly basis, as required.

Following these points doesn't just help with a due diligence defence, it will also help the company meet its legal obligations concerning consumer products, and it makes commercial sense to ensure that only safe products make it to market and that product safety incidents can be dealt with minimal impact to the business.

Dates for the diary

- | | |
|---------------------|---|
| 13 June 2017 | Radio Equipment Directive fully in force. All products falling under the new definition of "radio equipment" that are placed on the market from this date should comply with the new directive – save that the UK has confused the situation by not yet implementing the Directive into UK law. |
| 15 July 2017 | Government response expected to consultation on safe use of drones in the UK. |
-

Regulated Procurement



Catherine Wolfenden

Partner

T: +44 117 917 3600

catherine.wolfenden@osborneclarke.com

Current issues

New test for damages claims

The Supreme Court has **held** that there is a positive obligation on claimants claiming damages in public procurement challenges to show that the breach by the relevant contracting authority is 'sufficiently serious'. This means that the bar for a damages claim is now arguably higher than it was previously. However, as it stands from this case, any breach of the Public Contracts Regulations 2015 that results in the failure to award to the most economically advantageous tender will be regarded as a 'sufficiently serious' breach. One potential outcome of this change is that the courts may be more willing to allow the automatic suspension of contract signature (prohibiting a contract from being signed once a claim form has been issued) to remain in place. The decision flows from a case in which the UK government's Nuclear Decommissioning Authority settled claims brought by unsuccessful bidders for a £6.1bn nuclear decommissioning contract, paying £100m in damages and legal costs. An independent inquiry into the handling of the procurement and subsequent litigation will be conducted, with the report expected in October 2017.

Access to UK public contracts immediately following Brexit

A potential immediate consequence of Brexit may be that UK contracting authorities could seek to give preferential treatment to UK businesses. Suppliers without a UK place of business may want to consider taking steps to enable them to continue to bid for UK contracts immediately following Brexit. We suggest suppliers without an existing UK supply base may want to seek legal advice to consider available options.

Increased transparency and disclosure

Two recent cases and a new Procurement Policy Note issued by the Government have placed greater onus on contracting authorities to proactively disclose information that may previously have been withheld on the grounds of commercial confidentiality.

The decision in the case of *Bombardier v Merseytravel* [2017] EWHC 726 held that unsuccessful bidders are entitled to fully investigate the winning bid for evidence of breaches of procurement regulations. This followed the recent decision by the Information Commissioner's Office (ICO) regarding a request for information under the Environmental Information Regulations to Gloucestershire County Council (EA/2015/0254-6). The ICO allowed commercially sensitive aspects of a final contract to be disclosed to the complainants on the basis that disclosure was in the public interest. These developments mean that, when bidding in public procurements for public contracts, tenderers should make clear to contracting authorities that information contained in their bids is confidential and commercially sensitive, and should be prepared to engage with contracting authorities to resist disclosure of their bids, and the final signed contract, to their competitors.

Consultation on single source defence contracts regime

The Single Source Contracts Regulations 2014 apply to contracts between the Ministry of Defence and prime contractors, and to contracts between prime contractors and sub-contractors, where the contract has been awarded by the MoD without any competition and the value is over the relevant threshold. The Single Source Regulations Office is the body tasked with overseeing the application of Regulations. In March 2017, SSRO concluded a consultation on changes to the regulations, proposing to broaden their scope to include amendments to existing contracts, and to lower the threshold for qualifying sub-contracts. SSRO's final recommendations are expected to be published in June 2017 and will then be considered by the Secretary of State for Defence, with a likely implementation date of early 2018.

In focus: Personal liability

There are no offences carrying personal liability under procurement regulations in the UK. However, the convictions of employees or members may result in a supplier being excluded from participating in public procurements.

What is the risk?

If any individual member of a bidder's administration or management, or any individual with powers of representation, decision or control over the organisation, has been convicted of an offence, that supplier could be excluded from participating in public procurements. Applicable offences are listed in the regulations (the Public Contract Regulations 2015 and the Utilities Contracts Regulations 2016) and essentially encompass all offences carrying personal liability discussed throughout this edition of the Regulatory Outlook (such as bribery and fraud).

A bidder may also risk exclusion in circumstances where it is a requirement for it to employ individuals with professional registrations (such as accountants or company secretaries) and where, following those individuals being struck off, the supplier no longer meets this requirement.

Why is this relevant?

For companies that rely on contracts with public bodies or regulated utilities in the UK and across the EU, the financial impact of being excluded from participating in regulated procurements could be devastating. The exclusions apply to all regulated procurements in the UK and across the EU. Contracting authorities/utilities have no discretion in applying the exclusion. A supplier could find itself unable to win any new contracts until either it has taken 'self-cleaning measures' (see below) or the individual(s) concerned no longer retains a connection to the supplier.

What steps can be taken to mitigate the risk?

The regulations allow suppliers to 'self-clean' if they find themselves impacted by the personal liability of an individual. A bidder will need to provide evidence demonstrating its reliability despite the existence of a ground for exclusion. This is likely to include evidence of:

- implementing concrete technical, organisational and personnel measures to prevent further criminal offences or misconduct;
- actively collaborating with investigating authorities; and
- having paid compensation to those affected by the criminal offence or misconduct.

EU certificates

Some EU countries require bidders to provide certificates as proof that they and their members are free from criminal convictions. While a bidder can provide DBS certificates for individuals, there is no company equivalent available in the UK. Some countries will accept a sworn declaration, but this is not always acceptable. Bidders should clarify requirements well in advance of submitting tenders and seek legal advice if necessary

Dates for the diary

October 2017 An independent inquiry into the UK Government's handling of the procurement process for the £6.1bn Nuclear Decommissioning Authority contract is being set up and will be led by Mr Steve Holliday, former Chief Executive of National Grid. The inquiry will examine all aspects of the procurement process and subsequent litigation, the actions and conduct of the NDA and Government, and the extent to which assurance processes were effective. The report is due to be made available to the House of Commons and the Business, Energy and Industrial Strategy Select Committee in October 2017. It is expected to make recommendations and may result in further investigations and/or disciplinary proceedings.

Autumn 2017 The CJEU is expected to rule on whether bidders are under a duty to disclose economic links to each other to the contracting authority when bidding in the same procurement. The question was referred by the Lithuanian national court and considers whether related bidders are genuinely in competition (i.e. are they engaged in a 'pretence of competition'?) and the extent to which the contracting authority must bear the risks of such pretence if the duty to disclose is not set out in the procurement documents (Case C-531/16).

Spring 2018 The CJEU is expected to rule on whether the failure to provide a performance bond in a procurement can result in exclusion from a procurement. The Advocate General gave an opinion that a performance bond could be a valid selection criterion. However, this position has been criticised by commentators, who argue such a ruling may be incompatible with competition law. The AG's opinion offers guidance to the CJEU and may be followed or rejected (Case C-76/16).

© Osborne Clarke LLP
July 2017
Publication number
34459972

