

January 24, 2019

UK EMPLOYMENT UPDATE - JANUARY 2019

To Our Clients and Friends:

In this, our 2018 end of year alert, we look back at key developments in UK employment law over the past twelve months and look forward to anticipated key developments in the year ahead.

A brief overview of developments and key cases from 2018 which we believe will be of interest to our clients is provided below, with more detailed information on each topic available by clicking on the links to the appendix.

1. **Employment Status** (*click on link*)

We consider recent developments in the law regarding 'worker status' in the UK and look at how the Government responded to recommendations on employment status made in the Taylor Review in its Good Work Plan.

2. **Good Work Plan** (*click on link*)

The Government's Good Work Plan sets out a number of proposed reforms to UK employment laws and policy changes to ensure that workers can access fair and decent work, that both employers and workers have the clarity they need to understand their employment relationships, and that the enforcement system is fair and fit for purpose. We consider these below.

3. **Vicarious Liability** (*click on link*)

We consider the impact of two recent decisions of the UK Court of Appeal which look at vicarious liability in both the legal spheres of Employment and Data Protection. In relation to Employment, it was held that there was a sufficient connection between a managing director's job and his drunken assault on an employee to render the company vicariously liable for his actions. With regards to Data Protection, it was held that an employer was vicariously liable for the criminal actions of an employee who leaked the personal data of almost 100,000 employees, notwithstanding that the employer was held to have taken appropriate steps to mitigate the risk of such criminal actions occurring, and that the employee's actions were undertaken with the express intention of causing damage to the employer.

4. **Sexual Harassment and #metoo** (*click on link*)

The #metoo movement has had a significant impact on the use of non-disclosure agreements ("NDAs") in situations involving allegations of sexual harassment. We consider the circumstances in which it remains appropriate to use NDAs in connection with the settlement of such claims and allegations.

5. Data Protection *(click on link)*

More than six months have now passed since the General Data Protection Regulation (the "GDPR") became effective in May 2018. Given the potentially significant fines for non-compliance, businesses subject to the GDPR have been investing heavily in GDPR compliance programmes. However, uncertainty still surrounds the GDPR and how it should operate in practice. We consider the enforcement action taken by the Information Commissioner's Office (the "ICO") during 2018 and the approach the ICO has said it intends to take with respect to enforcement in the future. We also consider recent guidance on the territorial scope of the GDPR as well as the implications of Brexit on the European and UK data protection regimes.

6. Other News and Areas to Watch *(click on link)*

APPENDIX

1. Employment Status

The question of employment status has vexed the UK courts in recent years. Employment law in the UK is unusual in that it recognises three different ways of working: (i) as an employee under a contract of employment; (ii) as an individual who may not be classed as an employee but who otherwise provides services personally in circumstances which may attract 'worker' status; and (iii) finally, as a self-employed independent contractor providing services to a client. The distinction between these three categories has been called into question in a spate of recent cases, some involving the gig economy. We previously considered the different employment rights afforded to individuals in these three categories of working relationship in a [prior alert](#).

This year, the eagerly awaited judgment from the UK Supreme Court in the case of *Pimlico Plumbers Ltd and another v Smith* [2018] UKSC 29 gave further guidance on the approach to be taken by the UK courts when determining whether an individual who performs services for a client but who is not an employee should nevertheless enjoy protection under UK law as a 'worker'. As we indicated in our previous alert, the obligation to perform services personally is a necessary requirement for 'worker' status. When considering this issue, the UK Supreme Court highlighted the need to consider the terms of the contract between the parties in full (such that a contractual right of substitution in the Pimlico Plumbers contract was overridden by other clauses of the contract which indicated that the services were to be performed personally). Other relevant factors which contributed to the finding of 'worker' status in this case were tight control over the plumber's attire and administrative aspects of his job, onerous terms as to amount and timing of payment, and a suite of covenants restricting the plumber's working activities following termination.

As a consequence, care should be taken when engaging an independent contractor to ensure that the arrangements are documented clearly and that the terms of engagement (whether individually or taken as a whole) are not consistent with worker status.

2. Good Work Plan

The Good Work Plan, published in December 2018, builds on the response given by the Government in relation to the Taylor Review in February 2018, and reports on the progress of the issues raised in various consultations. In it, the Government responds to recommendations on employment status made in the Taylor Review by promising to (i) "*bring forward detailed proposals*" on how the employment status framework for employment rights and tax should be aligned, and (ii) provide legislation to "*improve the clarity*" of the employment status tests, "*reflecting the reality of modern working practices*". Unfortunately, however, no further information has been given about what this will entail.

The Government has also laid down three statutory instruments implementing the Good Work Plan that will become effective from 6 April 2020 and which: (i) provide that the written statement of employment particulars must be given from day one of employment; (ii) change the rules for calculating a week's pay for holiday pay purposes, increasing the reference period for variable pay from 12 weeks to 52 weeks; (iii) abolish a perceived loophole known as the *Swedish Derogation*, which allows agency workers to be paid less than if they were directly hired provided they have a contract of employment with the agency and are paid between assignments; (iv) extend the right to a written statement to workers (previously just employees); and (v) lower the percentage required for a valid employee request for the employer to negotiate an agreement on informing and consulting its employees from 10% to 2% (while keeping the minimum 15-employee threshold for initiating proceedings in place). From April 2019, the limit on financial penalties for breaches of employment law which have aggravating factors will be increased from £5,000 to £20,000.

3. Vicarious Liability Update

As reported [previously](#), the boundaries of the law on vicarious liability, which determines the circumstances in which an employer will be deemed liable for the acts of its officers and employees, continue to expand. We highlight below two recent decisions of the UK Court of Appeal in the field of vicarious liability:

3.1 *Vicarious Liability and Employment:* Overturning a decision by the UK High Court, the UK Court of Appeal held that a company was vicariously liable for an assault carried out by the managing director on another employee. In *Bellman v Northampton Recruitment Ltd [2018] EWCA Civ 2214*, the managing director punched an employee several times at an unscheduled drinking session after the office Christmas party. The UK Court of Appeal confirmed that, when considering the issue of vicarious liability, the UK courts should focus on the "*field of activities*" assigned to the perpetrator and ask whether the actions for which the employer is claimed to be vicariously liable fell within his or her "*field of activities*". In the present case, the managing director's seniority and the way in which he asserted that authority at the event at which the assault took place were both significant factors leading the court to conclude that the employer was responsible for the assault which he carried out at an unofficial out-of-office event.

This decision restores the UK Supreme Court's broader application of the "*close connection*" test to incidents of assault by an employee in *Mohamud v WM Morrison Supermarkets Plc [2016] UKSC* which we reported on [previously](#).

3.2 Vicarious Liability and Data Protection: In a decision that is likely to have far-reaching consequences for employers, the UK Court of Appeal upheld a controversial UK High Court judgment that an employer, Morrisons Plc, was vicariously liable for the criminal actions of an employee, notwithstanding that it had taken appropriate steps to mitigate the risk of such actions occurring. In the first group litigation after a data breach in the UK, Morrisons is liable in damages to over 5,000 individuals.

A disgruntled employee of Morrisons leaked the personal details of almost 100,000 employees to the internet. The UK High Court found that Morrisons was not directly liable for the breaches of the Data Protection Act 1998 (the "**DPA 1998**"), which has since been superseded by the GDPR and the Data Protection Act 2018 (the "**DPA 2018**") (which sits alongside the GDPR in the UK and, amongst other things, confirms the UK's approach to certain flexibilities and exemptions permitted by the GDPR), misuse of private information, and/or breaches of confidence. However, it found that Morrisons was vicariously liable for the employee's actions. Morrisons appealed to the UK Court of Appeal, however, the appeal was dismissed. The UK Court of Appeal held that (i) it was not implicit that Parliament had intended to exclude vicarious liability from the scope of the DPA 1998 and (ii) the UK High Court had been correct to find that there had been a "*seamless and continuous sequence*" of events between the breach and the employment relationship. The misuse of the personal data by the employee in this case was found to be within his "*field of activities*" as there was an "*unbroken chain*" of events between his work activities and the data leak. Referring to the decision in *Bellman*, the UK Court of Appeal said it also made no difference that the tort took place away from the workplace.

What this means for employers: The UK Court of Appeal's judgment, whilst concerned with the provisions of the DPA 1998, applies equally to the equivalent duties and responsibilities under the GDPR. In particular, in order to mitigate vicarious liability risks it may not be sufficient for UK employers to simply comply with their obligation under the GDPR to implement "appropriate technical and organisational measures" to ensure that personal data in their possession is appropriately secured. Hence, employers should also consider appropriate insurance coverage, whether by public liability policy or a bespoke cyber insurance policy. It remains to be seen how effective these policies will be, and they are unlikely to cover the entire exposure.

4. Sexual Harassment and the #metoo Movement

The #metoo movement has increased the social and political pressure upon UK employers to tackle issues of sexual harassment head on, particularly where perpetrated by those in authority. While settlement agreements and associated non-disclosure provisions remain both useful and appropriate when resolving employment disputes, care must be taken in situations involving allegations of sexual harassment, especially where those allegations have been upheld against the perpetrator or continue to be maintained by the alleged victim.

In particular, the use of NDAs or settlement agreements to prevent an employee from repeating, publishing or reporting allegations of sexual harassment has been called into question over the last year. The Women and Equalities Committee of the UK Parliament ("**WEC**") conducted an Inquiry into Sexual Harassment in the Workplace (the "**Inquiry**") in 2018, highlighting five points in respect of which they

called upon the Government to take action: (i) putting sexual harassment at the top of the agenda; (ii) requiring regulators to take a more active role; (iii) making enforcement processes work better for employees; (iv) cleaning up the use of NDAs, and (v) collecting more robust data.

The Solicitors Regulation Authority (the "SRA") subsequently issued a Warning Notice reminding lawyers that NDAs must not: (i) prevent anyone from notifying regulators or law enforcement agencies, of conduct which might otherwise be reportable; (ii) improperly threaten litigation, or (iii) prevent someone who has entered into an NDA from keeping or receiving a copy of the NDA. Further, in December, the UK Government responded to the Inquiry and said that a statutory code of practice on sexual harassment should be introduced, and acknowledged that NDAs require better regulation. The Government committed to consult on how best to achieve this and enforce any new provisions, but noted the lack of data and research on this issue. As a result, in November 2018, the WEC launched a new inquiry into the wider use of NDAs in cases where any form of harassment or discrimination is alleged. The findings of this are expected in Spring 2019.

In the circumstances, and while settlement agreements containing non-disclosure provisions remain a lawful and appropriate means by which UK employers can resolve disputes in which allegations of sexual harassment have been made, care should be taken to ensure that: (i) NDAs are not used in circumstances in which the subject of the NDA may feel unable to notify regulators or law enforcement agencies of conduct which might otherwise be reportable; (ii) lawyers do not fail to notify the SRA of misconduct, or a serious breach of regulatory requirements, and (iii) lawyers do not use NDAs as a means of improperly threatening litigation or other adverse consequences.

5. Data Protection

5.1 **Enforcement:** In a recent speech, the UK's Information Commissioner revealed that the number of complaints the ICO has received from the public regarding their personal data has increased from 19,000 since the GDPR came into effect, compared to 9,000 in a comparable period predating the GDPR. There have also been more breach reports – more than 8,000 since the GDPR came into effect and reports became mandatory in certain circumstances. The ICO's headcount has also increased to almost 700, which is 60% higher than in 2016.

These increases in complaints and resources have yet to result in increased enforcement action. The ICO has issued one enforcement notice, requiring the deletion of data subjects' personal data by the entity in default. This enforcement action is notable because it was taken against a Canadian entity and so demonstrates that the ICO will take action against foreign entities which are subject to the GDPR. More recently, the ICO has issued monetary penalties to organisations across the finance, manufacturing and business services sectors for non-payment of the data protection fees all data controllers are required to pay unless certain exemptions apply.

The ICO has not yet issued an administrative fine for a breach of the GDPR or DPA 2018. It has however recently imposed the maximum possible fine on an organisation under the DPA 1998, and in doing so indicated that the fine would have been significantly higher had the GDPR been in force when the breach occurred.

The ICO has produced a draft Regulatory Action Policy, which sets out the approach the ICO intends to take with respect to enforcement. Although this policy remains subject to Parliamentary approval, organisations regulated by the ICO will be relieved to hear that although the ICO will consider each case on its merits, as a general principle it is the more serious, high-impact, intentional, wilful, neglectful or repeated breaches that can expect to attract stronger regulatory action, and so they are unlikely to attract the highest administrative fines if they have taken sensible and appropriate measures to comply with the GDPR and the DPA 2018.

5.2 Territorial Scope: The GDPR has extraterritorial effect, and may apply both to organisations established in the EU and to organisations not established in the EU. Where an organisation is established in the EU, the GDPR applies to the processing of personal data in the context of the EU establishment's activities, regardless of where the processing takes place. Where an organisation is not established in the EU, the GDPR applies to processing activities relating to the offering of goods or services to or the monitoring of the behaviour of individuals located in the EU.

The European Data Protection Board (the "**EDPB**"), an EU body which is made up of the head of each European data protection authority and the European Data Protection Supervisor (the EU's independent data protection authority) (and which is tasked, amongst other things, with ensuring consistent application of the GDPR across the EU) has recently issued [guidelines](#) (currently subject to public consultation) on the territorial application of the GDPR, which are intended to provide clarity as to how the GDPR applies in practice. We have set out below some items of particular interest:

5.2.1 The meaning of "Establishment": An establishment implies the real and effective exercise of an activity through stable arrangements. The EDPB has confirmed that in some circumstances the presence of a single employee or agent in the EU may be sufficient to constitute a stable arrangement. However, the notion of establishment has its limits, and it is not possible to conclude that an organisation is established in the EU merely because its website is accessible in the EU. In addition, the EDPB does not deem a data processor in the EU to be an establishment of a data controller merely by virtue of its status as a data processor.

5.2.2 Data controller-data processor arrangements: Where an organisation subject to the GDPR uses a data processor which is not subject to the GDPR (for example, because that processor is not established in the EU), it will need to ensure that it puts in place a contract with the data processor which complies with the requirements of Article 28 of the GDPR. The processor will thereby become indirectly subject to some obligations under the GDPR. Where an organisation subject to the GDPR acts as a data processor, processing personal data on behalf of a data controller not subject to the GDPR, it will similarly need to ensure that it puts in place a contract with the data controller which complies with the requirements of Article 28 of the GDPR (save insofar as they relate to the provision of assistance to the controller in complying with the controller's obligations under the GDPR).

5.2.3 "Targeting" data subjects in the EU: An organisation which is not otherwise established in the EU will not become subject to the GDPR merely because it processes the personal data of individuals in the EU; an element of "targeting" those individuals must also be present, such that it is apparent that the organisation envisages offering goods or services to data subjects in the EU. Factors to be considered in

this regard include (amongst others) whether the EU or an EU member state is mentioned in connection with the goods or services, whether the organisation uses a language or currency which is not used in its home country but which is used in the EU, and whether the organisation offers the delivery of goods in the EU. This concept of "intention to target" is not relevant to the application of the GDPR with regard to the monitoring of data subjects' behaviour in the EU – such monitoring may be subject to the GDPR irrespective of any intention (or absence thereof) to do so.

5.3 *GDPR and Brexit:* On the day the UK leaves the EU, the GDPR will be transposed into UK law as domestic legislation. This means that data protection standards in the UK will not change dramatically after Brexit, at least initially. However, Brexit may affect the way in which the GDPR applies to businesses, and certain businesses may find themselves subject to both the "UK GDPR" and the GDPR proper, depending on the nature and structure of their European operations.

Separately, Brexit will have ramifications for personal data transfers, and particularly transfers from the EU to the UK. Currently, there are no restrictions on such data transfers. However, if the UK leaves the EU without the European Commission ("EC") having formally recognised its data protection laws as adequate, whether as a result of a no-deal Brexit or simply the failure to make an adequacy decision by the end of any transition period, and in the absence of any applicable derogation, adequate safeguards would need to be put in place in respect of any personal data transfers from the EU to the UK. This would typically involve the transferor and recipient entities entering into model clauses approved by the EC, although other options are available.

6. Other news and areas to watch

6.1 *Brexit:* Whilst it is impossible to predict, at the date of writing, how Brexit will unfold, we can say that Brexit is not expected to have a substantial impact upon employment rights in the UK for the moment, irrespective of the form it takes. A white paper issued in July 2018 by the UK Government indicated that there is no intention to repeal or amend employment or equality laws in the UK, including those which derive from or implement European employment laws. The paper states: "*existing workers' rights enjoyed under EU law will continue to be available in UK law at the day of the withdrawal*" and proposed that the UK will commit to a "*non-regression of labour standards*" in order to maintain a strong trading relationship with the EU.

Possible areas for reform post-Brexit could include compensation limits in discrimination claims (which are currently uncapped), as well as provisions for the accrual of statutory vacation and calculation of statutory vacation pay. We are happy to answer any questions which clients may have relating to Brexit and employment law.

6.2 *Simplification of tax on termination payments:* Since 6 April 2018, any payment in lieu of notice (including a non-contractual payment) has been treated as earnings and subject to tax and class 1 National Insurance Contributions ("NICs"). However, from 6 April 2020, all termination payments above the £30,000 threshold will be subject to class 1A NICs (employer liability only).

6.3 *Large and medium sized companies engaging workers through PSCs are to become responsible for PAYE and NICs:* In a move that will significantly impact those large and medium-sized companies

engaging workers via personal services companies ("PSCs") from April 2020, the responsibility for operating off-payroll working rules, and deducting any tax and NICs due, will move from individuals to the organisation, agency or other third party paying an individual's PSC. Organisations will have to reconsider whether there is any material benefit in using PSC structures for their indirectly engaged workforce as opposed to directly engaged self-employed contractors.

6.4 Pay reporting: A new set of regulations that came into force on 1 January 2019 bring in mandatory reporting of the ratio between CEO pay, including all elements of remuneration, and average staff pay for UK incorporated companies that are listed on the London Stock Exchange, an exchange in an EEA member state, the New York Stock Exchange or NASDAQ, and have an average number of UK employees above 250 in their group, all of which will be effective for accounting periods beginning on or after 1 January 2019. Further, the Government launched a consultation on ethnicity pay reporting, looking in particular at the sort of information that employers should be required to publish.



Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these and other developments. Please feel free to contact the Gibson Dunn lawyer with whom you usually work or the following members of the Labor and Employment team in the firm's London office:

James A. Cox (+44 (0)20 7071 4250, jacox@gibsondunn.com)

Georgia Derbyshire (+44 (0)20 7071 4013, gderbyshire@gibsondunn.com)

Heather Gibbons (+44 (0)20 7071 4127, hgibbons@gibsondunn.com)

Sarika Rabheru (+44 (0)20 7071 4267, srabheru@gibsondunn.com)

Thomas Weatherill (+44 (0)20 7071 4164, tweatherill@gibsondunn.com)

© 2019 Gibson, Dunn & Crutcher LLP

Attorney Advertising: The enclosed materials have been prepared for general informational purposes only and are not intended as legal advice.