Magrath Sheldrick Employment Insight

magrath sheldrick LLP
solicitors

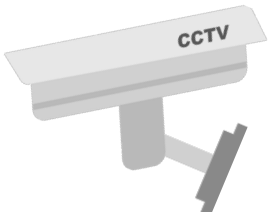
JUNE 2018

uk employment

In this edition

- Privacy in the Workplace
- Reflecting on GDPR
- Worker v Consultant Status Update
- Shared Parental Leave and Enhanced Maternity Pay
- Taxation Payments – PILON now Taxable
- Current Rates

PRIVACY IN THE WORKPLACE



Monitoring in the workplace is commonplace, with employers frequently monitoring staff email and internet usage, telephone calls and use of company devices. Many employers will also have surveillance cameras (such as CCTV) in place for security reasons or other purposes. Employers must ensure they comply with the applicable restrictions and requirements to protect their employees' privacy.

Businesses should be familiar with the data protection laws which apply in the UK, including the Data Protection Act 2018 (which implements the General Data Protection Regulation (which came into force in the UK on 25th May 2018)), Freedom of Information Act 2000 and the Protection of Freedoms Act 2012, as well as the Information Commissioner's Office Code of Practice for use of surveillance cameras ("the Code"). The Code makes clear that any response to Subject Access Requests ('SAR') or Freedom of Information requests must include surveillance footage. Meaning that footage needs to be accessible and kept for an appropriate period.

Recent judgments from the European Court of Human Rights ("ECtHR") have confirmed that employees have the right to a private life whilst at work, under Article 8 of the European Convention on Human Rights ("ECHR"). Article 8(2) ECHR allows this right to be interfered with only if the interference is legal and necessary, i.e. if it has a legitimate aim, and the ECtHR has repeatedly shown that a fair balance must be found between the employer's and employee's interests.

In Barbulescu v Romania 2017, the ECtHR ruled that there had not been sufficient warning given by the employer that Mr Barbulescu's personal instant messenger conversations on company computers would be monitored, or to what extent. The company's policy of expressly prohibiting all personal use of company computers was not sufficient to warn Mr Barbulescu that communications he did make about his private life would be accessible and monitored. The ECtHR said such monitoring was not permitted as employees have a reasonable expectation of privacy in all areas of the workplace. The ECtHR went further and confirmed that this right to privacy cannot be entirely removed by an employer's monitoring policies.

In acknowledging that employers need to be able to run their businesses effectively, which may necessarily involve monitoring employees, the ECtHR confirmed a case-by-case balancing exercise is required to ensure any monitoring policies are "accompanied by adequate and sufficient safeguards against abuse" considering that "proportionality and procedural guarantees against arbitrariness are essential". It set out guidance for domestic courts and employers to consider and assist them in avoiding breaching an employee's right to privacy:

(i) advance, clear notification to be provided to employees of any monitoring measures, together with methods of implementation;

(ii) details of the extent of monitoring procedures and the degree of intrusion into employees' privacy, including whether the content of communications are being monitored and any time limitations;

(iii) the employer's reasons for the monitoring which must be legitimate and justify the aims – noting that the more invasive the monitoring, the weightier the justification will need to be;

(iv) whether alternative, less intrusive, monitoring measures are possible;

(v) what the consequences of the monitoring are (for the employee subjected to it) and whether the actual use of the resulting data meets with the previously communicated aim;

(vi) does the employee have adequate safeguards against particularly intrusive monitoring which has not been previously notified.

With regard to the use of surveillance cameras to monitor employees, the ECtHR ruled in Antovic and anor v Montenegro 2017 that whilst the University of Montenegro lecturers were informed that video surveillance would be introduced, the stated purpose given by the University was not a legitimate aim. The University's stated reasons for introducing video surveillance included safety of property and people, and the surveillance of teaching. In Kopke v Germany, however, the ECtHR found that, preventing criminal activity may be a legitimate aim for covert surveillance by an employer.

In applying Barbulescu and Kopke in Antovic, the ECtHR said that the video surveillance of the lecturers amounted to a significant interference with their private social life because they could not avoid being recorded due to their contractual obligation to perform their duties where the surveillance was being carried out. This therefore required a legal and legitimate aim for the surveillance (under Article 8(2) ECHR), which could not be found. Monitoring teaching was held not to be a legitimate aim. Further, there was no evidence of risk to safety of property or people in the filmed areas and alternative monitoring methods had not been considered by the University.

In Lopez Ribalda and ors v Spain 2018, the ECtHR distinguished the covert use of surveillance cameras from the Kopke scenario on the basis that the latter case was targeted on specific employees suspected of theft and the surveillance was for a time-limited period (two weeks). Whilst Kopke shows that preventing criminal activity can be a legitimate aim for covert surveillance, the ECtHR ruled in Lopez that by filming all cashier staff throughout the entire working day without any limit on duration was disproportionate and did not strike a balance between the employees' Article 8 rights and the employer's interests. The level of intrusion into the employees' private social life was considerable because (as in Antovic) they could not avoid being filmed. Further, the fact that covert surveillance amounted to a breach of Spanish data protection law and guidance, and alternative surveillance methods were not considered, meant that it was not a justified monitoring method.

It is clear that employers need to consider their surveillance operations carefully. Whilst it can be temping (and often more convenient) to monitor continuously, this will almost certainly not be appropriate. Consider the need to operate cctv, the aim behind the monitoring and whether that need justifies the intrusion into the privacy of those working in the area. Importantly consider whether that stated aim can be achieved in a less intrusive manner. Employees will be more aware of their rights than ever following the implementation of the GDPR and employers are likely to see an increase in requests for personal data as a result, particularly from employees who are exiting on less than favourable terms.

REFLECTING ON GDPR

So, "GDPR day" passed and the world did not end! One mistake that many made in relation to the implementation of GDPR, was to panic about documenting compliance by the 25 May 2018 rather than focussing on understanding the wider obligations and overall goal of the long term protection of personal data. That panic resulted in data subjects receiving numerous emails attaching Privacy Notices in their various guises, the almost certain consequence of which being that the recipients did not read them – and so are none the wiser in relation to the information that the GDPR requires businesses to communicate!

The second mistake will be to assume that having got all the relevant ducks in a row, the GDPR project is complete! 'Job done', next project please! GDPR imposes ongoing data protection obligations, the need to audit and update compliance regimes, update and minimise data – ongoing maintenance will be required for businesses to remain compliant.

Personal Data is pervasive. Whilst client or customer data is frequently held in manageable silos, client files, customer records, accounts packages etc., this is not always the case. Indeed, it is rarely the case in relation to employees, where information about those employees stored by the business is likely to be held in a much more scattergun way. It is hard to think of a data location in a business where employee information will not be held. Various email folders and sub folders, business systems, back-up systems, accounts, payroll, personnel files, management information, inter-colleague emails etc etc etc. Consequently whilst many businesses have focused on their compliance obligations in relation to clients, customers, those on mailing lists and third parties, the greater risk to a business is likely (as is often the case) to be internal. A business is more likely to find itself reported to the Information Commissioner's Office (ICO) by a disgruntled employee than by a customer. Conflict breeds confrontation and with the significant amount of publicity around and the implementation of the GDPR, many employees will regard the ability to exercise their data rights or make a report to the Information Commissioner as a weapon to be used in achieving more favourable settlement terms on exit. Clearly no more the intention of the GDPR than the ability to use a subject access request as a pre-action fishing expedition was of the Data Protection Act 1998, but certainly a side effect.

Whilst some regarded the GDPR as a sledge hammer to crack a nut, some went into GDPR overdrive and others ignored it completely, many of the provisions are in fact simply good business practice, ensuring that the personal data of employees, clients and customers is properly protected. In a world where person data is becoming increasingly valuable and valued, the reputational risk of being seen to fail to protect personal data may well be catastrophic.

Many employers, particularly smaller ones without dedicated Data Protection Officers, or access to specialist advice have struggled with GDPR, including for some the concept of what is and what is not 'Personal Data'. Many have asked the question "does the fact that someone is simply named as being copied in an email, make that email their personal data which should be disclosed to them on request?" The short answer is unhelpfully, it depends! Whilst the email contains the name of a data subject (depending of course on the format of the email address), the information contained in the email may or may not be about them. If the email is generic and about third parties or business issues alone, is arguably not about the individual data subject and is therefore not disclosable on a subject access request. Sensible advice in relation to processing such personal data, must be to regard personal data as only as information relating to an identified (or identifiable) natural person and which it is about that natural person.

Key obligations in relation to employee data (in particular) include:

- Collecting and processing data fairly and lawfully – process data in a way that is reasonable, maintains confidentiality and in the way in which an individual will expect that data to be processed. Limit information and consider who needs to know what. Yes, tell a team that their colleague is absent by reason of illness – but do they really need to know what is wrong?

- Informing employees about the type of data held and how it is used (and then only using data for the purpose collected) – a properly drafted Privacy Notice provided to employees will achieve this. Ensure it is appropriately tailored and that the use of data is properly and accurately explained. Generic statements are to be avoided. Do not tell employees you monitor CCTV for building security or theft and then try to use that information to monitor time keeping and / or productivity.

- Keeping data up to date - remove extraneous and irrelevant information from personnel files, retain only information that is likely to be relevant in relation to the employee moving forward (including the event of litigation). Once someone has been working for you for a number of years and successfully performing their role – do you really need to retain their CV, in their maiden name with out of date information?

- Retaining data for no longer than is necessary – once an employee leaves the business and the risk of employment tribunal claims has passed, data should be minimised or deleted. An employee can bring a breach of contract claim any time up to 6 years after the date on which the alleged breach occurred. However, there can be no sensible reason for retaining data beyond that point (and much of the data on a personnel file will cease to have any relevance significantly earlier than that).

- Having appropriate Information Technology and Data Security measures in place to ensure that employee and client data is properly protected. Are all mobile devices encrypted? Are paper files permitted to be removed from the building? Do employees understand the consequences of breaching those policies?

- Granting employees access to correct or erase data – although in many instances, it will not be practicable to erase all data, particularly where there is obligation to retain the same for regulatory purposes. Remember the mantra – if you wouldn't want someone seeing it – don't write it down. Ensure that internal communications are appropriate – many a time has an employer tripped themselves up with inappropriate flippant comments on email!

- Ensure compliance cross boarder transfer restrictions. Consider how and when these may occur, when managers are travelling, where HR is based overseas, where recruitment processes involves screening undertaken by outside organisations that may or may not be based in the EEA.

What is clear is that Data Protection will continue to evolve. Anyone that regards their GDPR obligations as complete once the GDPR compliance file has been built and privacy notices sent out is missing the mark and does not understand the importance of properly protecting personal data.

Businesses will need to regularly review their compliance regimes, undertake appropriate audits when processing means and mechanisms change and regularly remind employees of their obligations in relation to personal data. Breaches will occur. It is fact of life that errors will be made, emails will be sent to the wrong person, data will be kept for longer than it should be and indeed businesses cannot sensibly believe anything else. The importance will be the processes you have in place to prevent the breach occurring in the first instance and, perhaps as importantly, how you deal with it once it occurs. Appropriate logs and notification procedures are vital as relevant training and guidance to a workforce. Sensible businesses are undertaking training on at least an annual basis and providing regular updates to the workforce – again logging that information to demonstrate compliance.

WORKER V CONSULTANT STATUS UPDATE

On 13 June 2018, the Supreme Court unanimously rejected the appeal from Pimlico Plumbers in Pimlico Plumbers Ltd v Smith. Many following this ongoing debate about worker status will recall that the case involved a plumber working for Pimlico Plumbers who claimed that he was a worker, rather than being self-employed. He was successful in the Employment Tribunal which found him to be a worker, and the Court of Appeal upheld the decision. This validation from the Supreme Court judgment will have important implications for gig economy, requiring employers operating in the 'gig economy' sector to carefully consider the employment of their workers.

Over the last few years, it has been hard to miss the flurry of cases concerning the blurred distinction between employees, workers and genuinely self-employed contractors, many of the cases dealing with issues arising in the so called "gig economy". The decisions have been leaning in favour of classifying individuals as workers, rather than self-employed contractors. Earlier this year, the Government set out its response to the Taylor Review which focused on the "gig economy" of part time and flexible workers. Unsurprisingly the Government confirmed that there is a lack of clarity around the different categories of worker and made various recommendations to try and resolve this!

Employers and commentators will be keeping an eye out for Uber decision, which is expected to be heard in the Court of Appeal later this year, following appeals from Uber after the Employment Appeal Tribunal confirmed that its drivers were workers, not self-employed contractors. Having now heard from the Supreme Court in Pimlico Plumbers, it seems likely that the Court of Appeal will dismiss Uber's appeal. However, that remains to be seen. The Employment Appeal Tribunal found that a driver for Addison Lee was a worker, and not a self-employed contractor in Addison Lee Limited v Gascoigne, so it will be interesting to see the direction Uber takes.

These decisions stress the importance of clearly defining the status of self-employed contractors. Most importantly they must be contractors in practice, as well as in name. It is clear that just stating that an individual is a "contractor" or "self-employed" in their contract is not sufficient.

Whilst there are a number of tests used by the courts to determine whether someone is a worker, the degree of control an employer has over when and how the individual operates is an important one. As is, the question of whether the employee is obliged to accept work when offered. Ultimately it will be a question of degree in each scenario – but it can be useful to consider how the outside world may view the individual.

SHARED PARENTAL LEAVE AND ENHANCED MATERNITY PAY

The Shared Parental Leave ('SPL') system allows new parents to share their leave entitlement following the birth or adoption of their child, with statutory pay entitlements set at the same rate as statutory maternity pay.

It is not uncommon for employers to pay enhanced pay to mothers on maternity leave over and above the statutory amounts. However, it is less common for employers to pay enhanced pay for SPL. Recent case law has helped to clarify the situation. In Capita Customer Management Ltd v Ali, the Employment Appeal Tribunal (EAT) confirmed that the failure of the company to pay a male employee enhanced shared parental pay, whilst paying female employees enhanced maternity pay, was not sex discrimination.

In this case, a new father wanted to commence his SPL following on from his initial two week paternity leave, for which he was paid in full. His employer had a policy which entitled female employees to 14 weeks full maternity pay following the birth of their child. Male employees were entitled to 2 weeks pay following the birth of a child. Mr Ali stated that the reason he wanted to take the SPL was to care for his daughter, as his wife was suffering with post natal depression and was medically advised to return to work. He claimed that he was dissuaded from taking this leave as he was told he would only receive statutory pay for that period, and that this was directly discriminatory on the grounds of sex. The reasoning for this was that he, as a man, wanted to care for his child and that he was not entitled to the same pay as a woman performing that role. The Employment Tribunal held that the claim for sex discrimination was successful. However, this was overturned on appeal by the EAT.

The EAT decided that it was wrong to determine that a woman on maternity leave was the proper comparator for Mr Ali. This is because purpose of maternity leave is for the benefit of the mother, not for the care of the child. The proper comparator would have been a woman seeking to take SPL. Therefore, it was not discriminatory on the grounds of sex to offer enhanced maternity pay to the mother but only statutory pay to the parent taking SPL.

However, the question of whether the same scenario could in fact constitute indirect sex discrimination (for example, the application of a provision, criterion or practice which disadvantages employees of a particular sex and cannot be objectively justified) has not yet been resolved, despite being considered in Hextall v Chief Constable of Leicestershire Police. Here, it was held that a failure to pay a man enhanced shared parental pay in line with enhanced maternity pay was not direct or indirect sex discrimination. On appeal, the Employment Appeal Tribunal found that the Tribunal made a number of errors when it was considering the indirect sex discrimination claim and the case has been remitted to another tribunal for it to be re-heard. Watch this space!

TAXATION PAYMENTS – PILON NOW TAXABLE

New tax rules apply to termination payments where employment terminates on or after 6 April. In short, the rules treat all employment contracts as though they contained a payment in lieu of notice ('PILON') clause irrespective of drafting. This means that basic pay the employee would have received during the notice period will now be taxed as earnings and therefore subject to income tax and employee's and employer's NI contributions. The calculation of portion of the termination payment on which tax is payable is based on a complex statutory formula. The upshot is that the new rules will mean that the previous loophole (where employees with contracts without PILON clauses could see notice paid tax free) has been closed. Many negotiated termination payments will now therefore cost employers more, which will need to be taken into account during termination discussions.

CURRENT RATES

National Living Wage

With effect from 1 April 2018, National Minimum Wage (and the National Living Wage) increased to £7.83 for those aged 25, £7.38 for those aged 21-24, £5.90 to those aged 18 - 20 and £4.20 for those aged below 18. It also rose to £3.70 for apprentices.

Redundancy

There has been an increase in the statutory redundancy pay rates, basic award for unfair dismissal and the maximum unfair dismissal compensatory award:

- The maximum amount of a week's pay for calculating statutory redundancy pay, and the basic award for unfair dismissal has increased from £489 to £508;
- The maximum statutory redundancy payment or basic award has increased from £14,670 to £15,240;
- The maximum compensatory award which can be made after a successful "ordinary" unfair dismissal claim has increased from £80,541 to £83,682 or one years salary, whichever is lower.

Parental pay and sick pay

April saw the usual rates increases for statutory parental pay rates (maternity, paternity, adoption, SPL) and sick pay. Parental pay for from 2018 – 2019 is £145.18, whilst statutory sick pay rate has increased to £92.05 per week.

For further information on any of the topics discussed in this briefing or wider employment or data protection issues please contact:

Chris Magrath (Senior Partner) chris.magrath@magrath.co.uk
Adele Martins (Partner) adele.martins@magrath.co.uk
Nichola Gallen-Friend (Partner) nichola.gallen-friend@magrath.co.uk