TAYLOR WALTON SOLICITORS

Aspire: helping owner and family managed businesses

Welcome to the Summer 2017 edition of the Aspire newsletter

In this edition of Aspire we look at some of the highlights of our work and developments in the law over the last couple of months. As well as looking at how to achieve success in litigation, we also discuss the importance of sales related terms and conditions, whether private complaints can be considered whistleblowing and the EU General Data Protection Regulation (GDPR).

I hope you enjoy this edition of Aspire. If you have any questions or suggestions for future topics for the newsletter, please do not hesitate to contact me, I would be delighted to hear from you.

Dermot Carey, Managing Partner of Taylor Walton

Clear and swift action delivers outcome in high profile litigation case

Taylor Walton's commercial litigation team are delighted to report our successful representation of Redbourn Group Ltd (Redbourn Group Ltd v Fairgate Development Ltd [2017] EWHC 1223 (TCC)), in a case that highlights the importance of appointing a solicitor who will act swiftly and decisively, and who can prepare comprehensive evidence and clear instructions.

Taylor Walton's proactive approach ensured a successful outcome for Redbourn Group where Saljuq Haider, one of our commercial litigation and dispute resolution solicitors acted on the case.

Background to the case

Fairgate Development Ltd (FDL) appointed Redbourn Group Ltd in February 2015 to act as the development and project manager for a proposed development. The contract ended in February 2016, with both sides claiming that the other had wrongly repudiated the contract. FDL complained about Redbourn Group's performance in a letter, dated 24 February 2016. Redbourn Group denied any failings in its performance and ultimately issued proceedings against FDL for damages.

The key practical issue highlighted by this case is the need for solicitors to act quickly and comprehensively in order to make an application to set aside a default judgment.

Our recommendations

This case demonstrates that clear and comprehensive instructions, and access to supporting evidence, is essential in order to be successful. Solicitors must make requests for extensions as soon as it becomes clear that the deadline will be missed, and ensure they meet the new deadline. Companies should be realistic and practical about how much time, and what resources, will be required.

The decisive and proactive actions of Saljuq Haider highlighted the weaknesses in FDL's evidence and its solicitors' (Debenhams Ottaway) procedural failings. Despite Saljuq's encouragement to act, and respect of the deadline extension, the defence team were on the back foot throughout this case with little chance to recover from Saljuq's clear and focussed demonstration of the deficiencies in their evidence and procedure.

Saljuq and the wider commercial litigation team at Taylor Walton are experts at helping their clients to achieve successful outcomes and resolve disputes. To find out more about how they work and how they can support your business, please visit taylorwalton.com, call Saljuq on 01582 731161 or email saljuq.haider@taylorwalton.co.uk

Selling to consumers: Can you rely on your terms?

Selling products and services over the internet, by telephone or mail order to consumers can cause unnecessary headaches (usually 'legally' induced).

Consumer regulation is updated regularly and provides extensive protections to consumer purchasers.

Many businesses have still to adopt new terms of sale in response to the Consumer Rights Act 2015 (and more worrying still, have not even incorporated the changes required by the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013).

Terms which have been left un-amended for a number of years run the risk of being unenforceable and attracting the unwanted attention of Trading Standards.

Perhaps the most important change has been in the cancellation rights of consumers:

Is the consumer given the correct period to cancel?

Any product, service or digital content which is sold to a consumer at a distance may be subject to a consumer's right to cancel.

The right to cancel is subject to some exceptions (such as for products which are made to measure or goods which will expire rapidly). Generally speaking however a consumer has 14 days to cancel a distance contract without giving a reason.

When the 14 day period starts to run will depend on what the consumer has ordered. For digital content and services the 14 day period will run from the date of order. For goods, the period will commence from the date on which all of the goods are delivered. As a good starting point, terms should be reviewed to check if the enhanced cancellation rights have been incorporated.

It is important to note that the right to cancel does not replace a consumer's broader rights in respect of faulty goods, services or digital content. Those wider rights set out when a business will be required to offer to replace, refund or repair a fault. However, unlike the right of cancellation, those rights do not need to be expressly set out in a business' terms of sale.

Stress testing your terms

Getting consumer terms right is no small task. Consumer protection regulations are extensive and guidance by regulatory bodies such as the Competition and Markets Authority is constantly refined. As a rule of good risk management it is advisable to keep as up to date with the area as is possible and to ensure your terms of sale are kept under regular review (annually is a good idea).

Mike Pettit is a partner and Head of the Commercial team at Taylor Walton. Mike can be contacted on 01582 731161 or by email on mike.pettit@taylorwalton.co.uk

ASPIRE SEMINAR PROGRAMME 2017:

The Banks of Mum, Dad, Grandma and Grandad
19 September 2017
4pm - 6pm, Beales Hotel, Hatfield

The New Pre-Action Protocol for Debt Claims
28 September 2017
4pm - 6pm, Beales Hotel, Hatfield

Book online at taylorwalton.com now
or email marketing@taylorwalton.co.uk for more details.

Is a complaint about a private workplace dispute "whistleblowing"?

The Court of Appeal in the case of Chesterton Global Ltd v Nurmohamed (the Chesterton case) has concluded that matters which are in the worker's private interests does not prevent the matter also being in the public interest. As a result employers should consider whether complaints made by employees about a private workplace matter are also protected disclosures ("whistleblowing").

What is Whistleblowing?

"Whistleblowing" is the common term given to a situation where an employee makes what is known legally as a "protected disclosure".

A protected disclosure is made where a worker discloses information about an organisation which is made in the public interest for example, breach of a legal obligation, criminal offences, concerns about health and safety practices. Workers who "blow the whistle" have, in certain circumstances, a right not to be dismissed or subjected to any other detriment as a result.

- Employees do not need to have 2 years' service in order to bring a claim that they have been dismissed for making a protected disclosure. It is often the case that an employee with less than 2 years' service will argue that they have "blown the whistle" in order to challenge their dismissal as they are not eligible to bring an ordinary unfair dismissal claim.
- A worker will be protected under the whistleblowing legislation where they make a disclosure which relates to specified kinds of malpractice. The disclosure could be made in an email, during a meeting or raised as part of a grievance. In addition, the disclosure does not have to relate to the employer's business and could concern a client or supplier.
- A worker who makes a disclosure will be protected where they have a reasonable belief in the disclosure and the disclosure is made in the public interest. If a worker can point to objective grounds to justify their belief, it does not matter that no legal obligation exists or the belief is based on incorrect facts.
- Although the legislation in this area is drafted to encourage workers to make disclosures internally, workers who make external disclosures will be protected in some circumstances. In particular, disclosures can be made to "prescribed persons" identified in legislation. Provided the worker believes the information is substantially true and concerns a matter within that person's remit, there is no need to tell the employer first. Employers should ensure that workers are aware that it is preferable to report matters internally in the first instance by putting appropriate policies and procedures in place to encourage employees to do so.

What is in the public interest?

In the recent Chesterton case the Court of Appeal considered this question:

- Mr Nurmohamed was employed as an estate agent and was paid commission along with 100 of his colleagues. He alleged his employer exaggerated its expenses in order to depress profits by £2-3million and thus reduce commission payments paid to him and his colleagues. He argued his allegation was a protected disclosure as he reasonably believed it was true and it was in the public interest to make the disclosure.

- Mr Nurmohamed was dismissed after he had made his disclosure and successfully claimed unfair dismissal on the grounds of whistleblowing.
- Chesterton Global appealed initially to the Employment Appeal Tribunal and subsequently to the Court of Appeal on the grounds that the allegation made by Mr Nurmohamed was not in the public interest.

The Court of Appeal in the Chesterton case found that Mr Nurmohamed's disclosure was in the public interest. The Court stated that the following factors would normally be relevant in determining whether a disclosure is in the public interest:

- The numbers in the group whose interests are affected by the disclosure;
- Whether the nature of the disclosure of wrongdoing is serious affecting a very important interest rather than a disclosure of a trivial wrongdoing;
- The disclosure should relate to deliberate wrongdoing rather than disclosure of inadvertent wrongdoing; and
- The identity of the alleged wrongdoer - the larger or more prominent the wrongdoer, the more likely the public interest will be engaged.

However, the Court of Appeal went on to state that Employment Tribunals should be cautious about finding that a worker making disclosure about a private workplace dispute is in the public interest. The broad intent behind the legislation is that workers making disclosures about private workplace disputes should not attract whistleblowing protection even when more than one worker is involved.

We now await further case law to find out how broadly the Chesterton case will be interpreted. In the meantime, employers are advised to ensure that they have suitable mechanisms in place so that concerns raised in the workplace are dealt with appropriately and to take legal advice before making decisions in relation to potential whistleblowing matters. Taylor Walton is able to advise employers on all aspects of whistleblowing and their potential liabilities in this complex area of employment law.

Alec Colson is a Partner in the Employment Law Department and can be contacted on 01582 731161 or by email alec.colson@taylorwalton.co.uk

Is your business ready for the GDPR?

The EU General Data Protection Regulation (the "GDPR"), was adopted on 25 May 2016. It repeals the current, less onerous, EU Data Protection Directive, and must be complied with by 25 May 2018. It has direct effect on all member states, so there is no requirement for national implementation laws. The Government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR, although it remains to be seen whether implementation will continue post-Brexit.

The GDPR broadens the reach of current legislation, enhances the rights of the individual (the "data subject") and introduces new rights.

Key rights of the individual

- Right of access – individuals will have the right to obtain confirmation that their data is being processed, and have access to that data;
- Right to rectification – individuals are entitled to have personal data rectified if it is inaccurate or incomplete, and must receive a response to any rectification request within one month;
- Right to erasure ("right to be forgotten") – an individual may request the deletion or removal of personal data where there is no compelling reason for its continued processing;
- Right to restrict processing – individuals are entitled to restrict further processing of their data. Their personal data may be stored, but not further processed.
- Right to data portability – individuals may obtain and reuse their personal data for their own purposes across different services;
- Right to object – individuals can object, amongst other things, to the processing of personal data for direct marketing purposes (including profiling), and in certain other circumstances too (such as research) where the individual objects on "grounds relating to his or her particular situation".

Assessing the risk

Most businesses will become accountable for measuring the level of risk that processing data will have on data subjects. This may require the appointment of a data protection officer.

Data protection impact assessments must be performed prior to any data processing requiring the use of new technologies, if that processing could cause a high risk to the data subjects. If it is revealed that the processing does, in fact, pose a high risk to the data subject, businesses are required to consult with their "supervisory authority" (see below) before any action is taken. Adequate risk assessment procedures should be set up as soon as possible, to ensure familiarisation with the new system prior to the GDPR becoming law.

Accountability

The GDPR requires businesses to demonstrate compliance. How you do so will depend largely on the size and nature of your business but, as a minimum, you should be prepared to maintain documentation such as records of internal audits of data processing activities and reviews of internal HR policies. Some businesses will be expected to implement internal data protection policies, and to carry out regular staff compliance training.

Consent

This area sees the biggest change to current protections for the individual. Consent to data processing must be freely given, specific, informed and unambiguous. There must be some form of clear affirmative action – a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and simple ways must be provided for people to withdraw consent. This is likely to severely restrict the ability of businesses to purchase personal data.

The rules are more stringent around consent of children. In most cases, the consent of the parent will be necessary.

A thorough review of how and when you obtain consent should be undertaken to ensure your business does not fall foul of the new regulation.

Supervisory authorities

Compliance with the GDPR will be overseen by a "supervisory authority", such as the Information Commissioner's Office in the UK. Since one of the GDPR's main aims is to harmonise data compliance throughout the EU, businesses who operate in more than one EU country will only be required to work with one "lead supervisory authority", determined by the location of their "main establishment" in the EU. This simplification will hopefully reduce the administrative burden on business.

Data Breach Notification

Businesses must notify their supervisory authority within 72 hours of a data breach - unless it is unlikely to create risk to the subject. This could prove to be administratively convoluted and costly. It is therefore imperative for businesses to have a breach response plan in place to ensure prompt compliance.

Fines

Every business that processes customer and other personal data needs to comply with the GDPR. There will be a significant increase in fines of up to 4% of annual worldwide turnover, or €20 million, for violating the data protection principles, conditions for consent or the rights of data subjects. Further fines of up to 2% of annual worldwide turnover or €10 million could be issued for breaches such as internal record keeping and breach notification. The ICO has increasingly shown a willingness to take enforcement action over data protection breaches, and this looks set to rise significantly.

It's not all doom and gloom

The GDPR is intended to make data protection more suitable for a modern environment. The introduction of a lead supervisory authority will be welcomed by those businesses with establishments in more than one EU country, and the GDPR will hopefully reduce the amount of redundant administrative tasks. However, the GDPR is primarily about empowering those whose data is on file. Due to the severity of the fines a business could face for a breach of the GDPR, it is imperative to review current data protection procedures and prepare to install new mechanisms where required.

To ensure your business is ready for the GDPR, contact Peter Kouwenberg in Taylor Walton's Commercial Team on 01582 731161 or by email at Peter.Kouwenberg@taylorwalton.co.uk.