SEPTEMBER 2017 // ISSUE 02

THE IN-HOUSE TRACK

Reviewing what matters for today's GCs

STEVENS&BOLTON

Stevens & Bolton has produced this magazine exclusively for GCs and their in-house teams, with the aim of providing strategic legal insight into the challenges, changes and opportunities facing the global business. We hope you will find The In-house Track a valuable resource which explores the important legal topics that impact in-house counsel the most.

In this, our second issue, we examine some of the critical legal challenges that global businesses face today. With Brexit rapidly approaching, we look at key issues businesses should now be actively addressing. We look at ways cyber-security can be managed as a fundamental part of the M&A process. With the ever shifting landscape of dispute resolution, we look at the factors to weigh up when choosing between litigation and arbitration in cross-border disputes. And with GDPR on the horizon, we look at the rules in practice and changes in approach to data management to ensure your business is ready for May 2018.

Beyond legal developments, we take a look at how to protect your company's brand identity and reputation; the cultural changes brought about by today's millennial lawyer and how to remain an agile business; and with ever evolving technologies, we examine the strategic impacts associated with "the fourth industrial revolution".... including Artificial Intelligence.

We hope that you find this edition of The In-House Track useful. This is your resource and we're keen that it becomes a key fixture on your reading list and addresses your information needs. We would welcome your feedback and any suggestions for future issues.

Richard King, Managing Partner
Tel: 01483 734242
richard.king@stevens-bolton.com

CONTENTS

04 Do look down: how to approach the Brexit cliff edge
What should in-house lawyers be thinking about now?

08 Talkin' 'Bout My Reputation
Regardless of the industry, reputation matters

10 Flex or fall behind?
How to remain an agile business in today's flexible working environment

12 GDPR: Too big to ignore
Time to ensure your business is ready for the changes coming down the track

16 M&A: Make sure cyber-security isn't your Achilles Heel
Time to prioritise cyber-security in M&A

18 The algorithm is gonna get you
AI, distribution and the law

22 Litigation v arbitration
Which is better when it comes to cross-border disputes?

DO LOOK DOWN: HOW TO APPROACH THE BREXIT CLIFF EDGE

At the time of writing, the government is releasing ‘key position papers’ and the ‘withdrawal bill’ is about to be debated in parliament.

It is 14 months after the decision to leave, and 19 months before the UK will most likely be out of the EU. Yet it feels like the government is nowhere near halfway through the process, despite the ‘cliff edge’ of withdrawal rapidly approaching.

Donna Harris, Director of Legal Services at Aviva, was widely reported as suggesting to the Law Society’s In-House Division in June that businesses should not ‘waste money on external Brexit advice right now’. This was on the basis that any advice would be too theoretical. Having spoken to a number of GCs and other in-house lawyers in the intervening period, that is a widely held view and a rational one, for the moment, in the case of many businesses and areas – although certainly not all.

In terms of how prepared you or your business is for Brexit, much will depend on the nature of the business you are advising. Some businesses are reported as having already suggested or indicated significant moves out of the UK, from banks, including Barclays, Deutchse Bank and Goldman Sachs, to others such as Easyjet, Diageo, and Microsoft.

If you work at an organisation looking at moving location then associated issues may already be taking up some of your time or resource. For the vast majority of businesses, though, Brexit planning is at a relatively early phase as we await concrete and actionable developments.

So, what should in-house lawyers be doing or thinking about now? As set out below this is a good time to develop what one might call a hard Brexit mindset, to get buy-in and budget and to start thinking carefully about the impact of Brexit on the day job.

Developing a hard Brexit mindset

No, this does not involve becoming more like Nigel Farage, but you do need to plan for a hard Brexit. This is a challenge. As the EU referendum demonstrated, it is very hard to invest time or even more money in a result that you do not expect and that you may not want (which I suspect will be the attitude of many in-house lawyers in the UK). The prudent approach at this stage is to assume there will be a cliff edge, and that the UK will fall off it on 29 March 2019. There may be a transitional period, or Brexit might not happen or be so watered down as to not lead to any practical challenges for most businesses but, as they say, if you fail to prepare, prepare to fail.

Get buy-in and budget

Resource required will be best procured by ensuring that senior managers are on board, so make sure you involve them and put them on notice. Part of this should include Brexit contingency planning. Budgets are currently being agreed or will shortly be agreed that will need to take your business to the point of exit from the EU - make sure that the legal team has the resource to stay active in this area. It may be worth considering the following:

- Will there be changes in the teams as a result of Brexit? Do you need to budget for recruitment (or redundancies)?
- More generally will there be immigration requirements and what will be the costs of these? It's worth carrying out an audit as to how many EEA nationals the business employs, as well as how many dependants of EEA nationals. Under the government's current proposal, EEA nationals who have been in the UK for five years as at an unconfirmed date will likely be able to apply for settled status. Even those who currently have Permanent Residence will apparently have to apply for settled status. These employees may require financial support with their applications, potentially including the cost of legal advice. Will the business cover that? Some EEA nationals who have already spent five years in the UK now may still want to apply for Permanent Residence as currently they can apply for naturalisation as a British citizen after holding permanent Residency status for 12 months. Others may want to apply for naturalisation shortly to ensure they have a British passport by March 2019.
- Will the business need to look at how it can attract British nationals if it currently relies heavily on EEA nationals? Will this lead to extra costs in the form of additional benefits or training? It is likely EEA nationals will have to apply under the Immigration Rules which apply to non-EEA nationals. In many cases the business will need to sponsor the individual. It's therefore essential to check that if the business has a sponsor licence all details are up to date and to avoid any risk that the licence is revoked for non-compliance. If in doubt consider an immigration audit.

Make sure that the legal team has the resource to stay active in this area

- Will you need to upskill in any particular areas, such as employment law, trade-related issues or to deal with changes to sector specific regulatory obligations?
- If your business is moving out of the UK to a certain extent, are you more likely to need local legal expertise from a different jurisdiction?
- Will you need emergency support and/or secondments from friendly law firms or other sources?
- Are there areas of your business that are particularly reliant on EU law, where litigation is likely following Brexit (for example due to uncertainties created by the withdrawal bill approach)?
- Are there pressing reasons for litigating prior to Brexit (for example, follow-on damages based on EU cases)?

Shifting your current legal analysis

When it comes to current legal issues, it's important to bear Brexit in mind. Frustration and force majeure may not be capable of being relied upon as a result of Brexit alone in the vast majority of cases. It is therefore sensible to be as clear as possible in contracts as to whether the UK's withdrawal from the EU is or is not a 'force majeure' event. The definition should be tailored accordingly, to remove any doubt.

Considering whether to include a price adjustment mechanism to take account of performance becoming more or less expensive following the UK's potential withdrawal from the EU is a good idea. Prices may alter because of changes to import/export tariffs, visa applications and other factors. Adjusting prices or switching currency may also be advisable if the applicable contractual currency crosses certain agreed thresholds.

Brexit-related factors could lead to termination - this might for example be a very big issue in finance agreements that rely on passporting rights. GCs should be considering this eventuality in relevant pre-existing agreements and in agreements being negotiated from now on to determine whether or not termination for Brexit should be allowed. It is essential to expressly state the agreed position.

Brexit will have an effect on specific dispute resolution procedures, such as arbitration. Including potential scenarios for disputes in each contract or agreement is likely to minimise the uncertainties surrounding the enforceability of judgments between the UK and remaining EU member states following the UK's possible withdrawal.

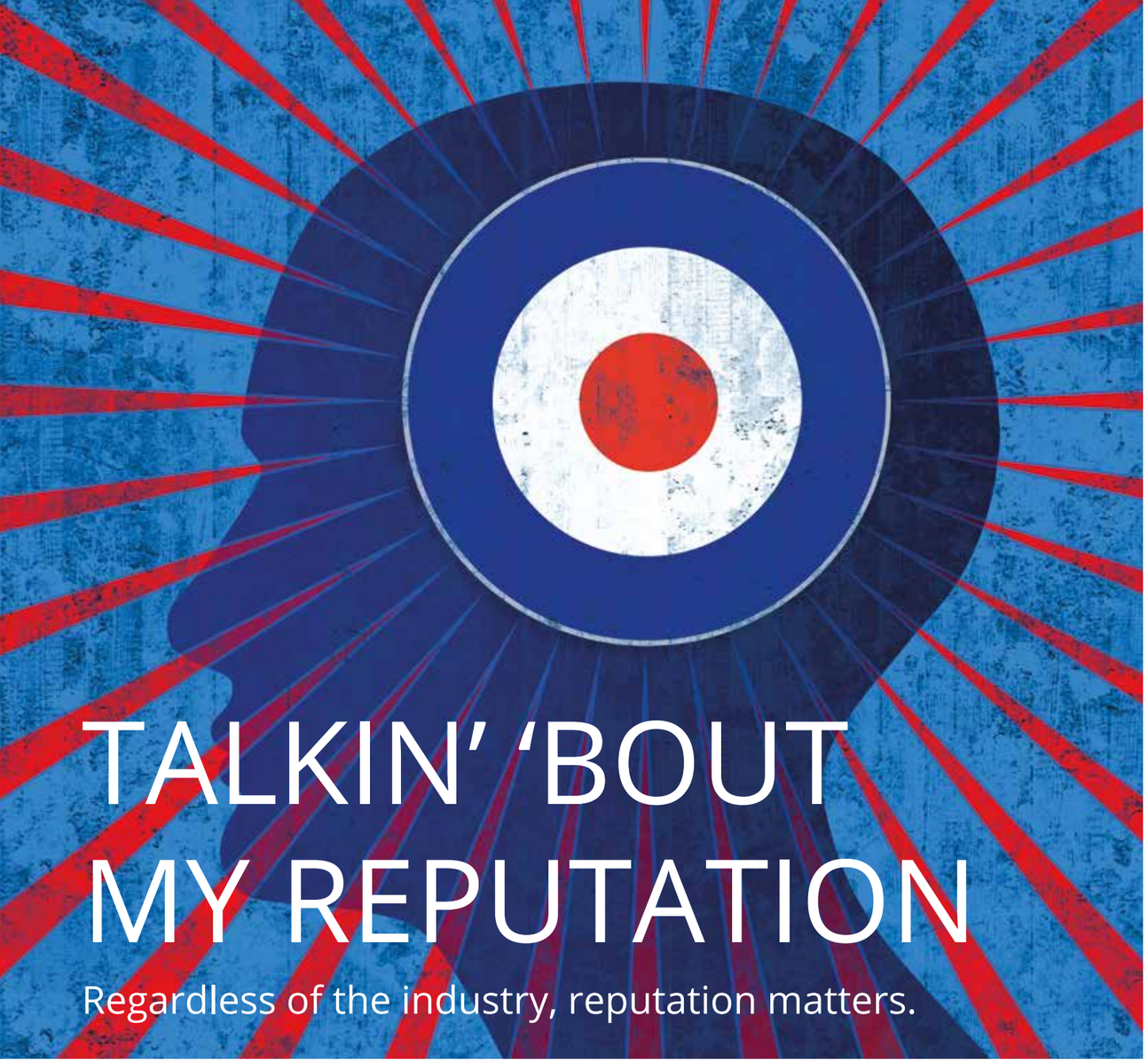
It goes without saying that GCs need to be analysing those contractual clauses referencing EU law, compliance with EU law and any changes to such law. You should decide which party is responsible for monitoring and ensuring compliance with particular laws and any changes in such laws, and which party bears the costs associated with this.

Data protection law is another area where it will pay to be on the front foot - for example there may be a change control clause to allow amendments following Brexit (this is likely to be particularly relevant where there are significant data privacy issues, such as in IT hosting contracts). The UK has suggested it will continue to abide by EU data protection law but may be reliant on an EU adequacy decision post-Brexit.

Finally, I would encourage all GCs to consider any implications in relation to Brexit in employment documentation. For example, any offer letters, employment contracts or secondment agreements should make it clear that the employment or secondment is conditional on the person continuing to have the right to work in the UK. If seconding a British national to an EU member state, consider what will happen if they no longer have the right to continue working in that country post-Brexit.

Clearly there is no certainty that the UK will fall off a Brexit cliff edge, that the UK will not secure an orderly transition, or that Brexit will in fact happen at all. But as lawyers our job is to help in the risk management process and as such we need to engage with this very considerable area of risk sooner rather than later.

Gustaf Duhs
Partner
01483 734217
gustaf.duhs@stevens-bolton.com



TALKIN' 'BOUT MY REPUTATION

Regardless of the industry, reputation matters.

Uber's ongoing challenges, which are many and varied, serve as a stark reminder to us all of the power of public perception. For most businesses, developing a strong brand identity and reputation is a priority. A distinct, recognisable brand is vital to growth and success; as consumers' decisions on purchasing goods or services rely on the associations that a brand conjures up.

However, protecting a brand can also be a minefield. Reputations take years to build, and yet are destroyed in moments; and even the way in which a business goes about brand protection can have a damaging effect on its brand.

"Who Are You?"

Thinking about your brand identity and reputation has to begin early, and ideally before a significant amount of money has been invested in design and marketing.

At the start of any brand development it is advisable to carry out clearance searches to ensure that no third party rights will be infringed once the brand launches. The approach taken at this stage will be very business-dependent. It's obviously possible to do some basic Google and domain name searches of the proposed name to identify potential issues. However, for companies that are going to rely heavily on their brand, particularly those with international ambitions, relying on such basic searches is not only risky, but potentially dangerous. Investing in professional advice and clearance searches at this stage can prove invaluable.

"Now It's A Legal Matter (baby)"

The most effective way to protect a logo or a brand name is by registering it as a trade mark in the jurisdictions in which the company is active. However, brand protection does not end with the first registration and needs to be considered at regular intervals, particularly if expansion into other markets is planned. GCs, who often have the task of coordinating this, need to ensure there is a good line of communication between the legal and marketing teams, to make sure new brands, sub-brands, product lines and other innovations are appropriately protected.

Additionally, whilst having a registered trade mark gives you legally enforceable rights, you can only enforce those rights if you are aware of infringements. Training employees to recognise and monitor infringements is critical, particularly for those in sales and marketing who are generally most aware of what competitors are doing.

One cheap and easy way is to sign up for internet alerts for any activity containing your brand name. There are also specific 'watch' services, which will monitor trade mark registries in relevant jurisdictions and flag any that might present a potential infringement.

"Won't Get Fooled Again"

Identifying infringements is important, but relatively straightforward compared to what comes next: deciding what to do about it.

Ideally, each infringement would be reviewed independently so that individual responses can be prepared. Smaller businesses will often find this easier as the number of infringements encountered is likely to be manageable. However, taking it further and enforcing rights can be expensive, and these same businesses might not be in a position to engage solicitors or issue court proceedings when they need to.

On the flip side, larger companies often take a more robust approach by rolling out a template response as a first step, almost regardless of the scale of the infringement, or the size of the recipient's business. This broad-brush approach often arises out of necessity; as a business grows, so does the number of infringements and the number of jurisdictions in which issues may arise, making it more difficult to manage a bespoke brand protection strategy.

"The Real Me"

Although the one-size-fits-all method can be an effective approach in terms of cost, it runs the risk of backfiring and damaging your brand with the bad publicity that can result. Media coverage in this area often adopts a David v Goliath narrative; it doesn't sit well with the public when the optics are of a big corporate going after small family-run or independent businesses. Numerous companies have suffered adverse publicity as a result of their own brand protection approach: Brewdog, Red Bull and Adidas, to name but a few recent examples.

The speed with which stories can go viral on social media heightens the risk even further. However, if monitored and used well, social media can also be one of the most effective antidotes. If the company concerned acts quickly, uses humour and shows humility then the situation can be diffused, and the damage minimised.

> *– it doesn't sit well with the public when the optics are of a big corporate going after a small family-run or independent business*

GCs are often the ones faced with the task of striking this balance. If, therefore, a one-size-fits-all-approach is adopted initially then it is important that there is an escalation procedure in place to allow intervention at the right point, to minimise the potential for damage caused by over-zealous enforcement.

"Who's Next?"

In summary then, a brand is not just a name. It's a valuable and ever-changing asset, which can require as much, if not more, care and attention than any other aspect of a business; so investing in it at the start and protecting it carefully for the future will never be wasted effort.

Tom Lingard
Partner
01483 406988
tom.lingard@stevens-bolton.com

Elaine O'Hare
Senior Associate
01483 401263
elaine.o'hare@stevens-bolton.com

FLEX OR FALL BEHIND?

With today's millennial lawyer more inspired by flexibility than pay, GCs must adapt to a change in long hours culture.

With a Brexit-led 'brain drain' potentially looming on the horizon, many GCs are feeling the pressure to bow to flexible working requests from their in house team in a bid to remain as attractive as possible to key talent. The change is in part, being driven by the new talent pool of millennial lawyers, who view flexibility around working hours as a benefit equal to pay. Technological advances have also played a role, making 'home' or 'agile' working increasingly accessible and affordable for businesses. Furthermore, a growing cohort of law firms are introducing agile working policies thereby increasing their appeal to the legal talent pool. Yet adopting such innovative working practices can pose challenges for today's GCs. How best to remain agile and what are the pitfalls to avoid?

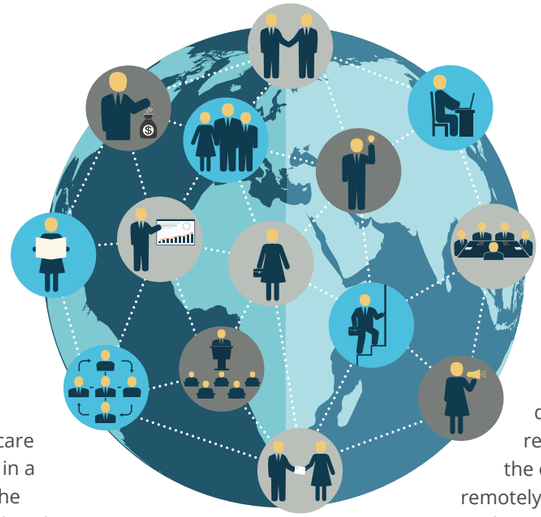
The letter of the law

The right to request flexible working was previously viewed as the preserve of working mothers or those with familial responsibilities and therefore out of reach for the majority of millennials. However, in 2014, the statutory framework changed and the floodgates were opened. All employees now have the right to request flexible working (subject to their having 26 weeks continuous service) and the catalyst for a request to change working pattern can now include anything from a wish to pursue a regular sporting activity, further education (which can be of no direct benefit to the business), or simply achieving a different work / life balance.

The statutory right to request a flexible working pattern is, of course, exactly that, and there is no statutory obligation for GCs to automatically grant a request from a team member to change their working pattern. Whilst the employer must meet with the employee to discuss how their proposal might work, they can rely on eight potentially fair reasons to reject a request which are enshrined in section 80 (G)1 of the Employment Rights Act 1996. These include the employer's inability to reorganise work amongst the team, detrimental impact on performance or inability to recruit additional staff.

The globalised and digitalised workplace makes flexible working patterns more easily accommodated

The statutory reasons are of course primarily business and/or role related. They do not assist GCs in fending off multiple or competing flexible working requests from their team. GCs can quickly reach a tipping point at which their team are viewed as a 'Marie Celeste' department where employees are physically invisible. Once saturation point is reached it can be difficult to avoid making social judgments in dealing with flexible working requests e.g. prioritising the request of the working mother who wishes to work 4 out of 5 days, over the man who wishes the identical pattern to surf once a week. Dealing with the request is often an exercise in risk management – assessing who is gifted the strongest discrimination claim if the application is rejected. Female employees seeking a working pattern to accommodate child care commitments will inevitably be in a stronger position legally, than the employee simply seeking to strike a better work / life balance. However, for many GCs the issue is a pragmatic and commercial negotiation – how much would it cost the business if I lost this individual, can I attract the right talent if I am intransigent on working hours?



Consistency isn't key

It's a common misconception that a consistent stance in rejecting all flexible working requests will 'gift' employers a defence i.e. a 'get out of jail free card'. Whilst many flexible working requests cite examples of a desired pattern working successfully elsewhere in the business, Tribunals expect employers to judge each application for flexible working on its merits, at the point in time it is made. This takes time and requires a deft hand.

Technology means it really can be business as usual

Technological advancement has played a key part in changing attitudes to flexible working. Inevitably some sectors lend themselves to flexible working more than others, however, GCs often cannot credibly argue a 'nervousness' relating to a loss of employee connectivity or a fear that employees will enter a communications vacuum if away from the office. Those arguments have largely disappeared given the ability to monitor employee output digitally, and the requirement that employees are contactable 24 hours a day. The reality is that most lawyers now walk around with their 'office', in the form of a smart phone, in their pocket. The globalised and digitalised workplace has led to a blurring of core or 'business' hours, which makes flexible working patterns more easily accommodated.

But, it is a balancing act...

Connectivity, of course, brings its own challenges in terms of how lawyers can be encouraged to 'switch off' and disengage from work so as to avoid burn out. However, rejecting a request because of concerns that the physically absent lawyer will miss those crucial 'coffee pot' conversations, a regular face to face meeting or ad hoc 'head round the door' questions, dissipate when the rest of the business is ahead of the curve and already working remotely. The statutory ground for rejecting the request - 'detrimental impact on performance' - simply does not hold water.

All this said, the challenges of flexible working are surmountable. GCs who embrace flexible working will inevitably have a competitive advantage in the recruitment market given that accommodating such patterns is viewed as a hallmark (and increasingly a hygiene factor) of workplace progression and innovation. Ultimately the future is flex or fall behind – the number of people working flexibly will soon surpass those that don't. The change has been driven by a generation who desire a career path that fits around their lives, and not the other way around.

KEY POINTS

- All employees with 26 weeks continuous service now have the right to request a flexible working pattern.
- Employers can rely on 8 potentially fair reasons to reject a request to work flexibly.
- Flexible working patterns are becoming common place and are more easily accommodated given technical advancements.

Hannah Ford
Partner
01483 401218
hannah.ford@stevens-bolton.com

GDPR: TOO BIG TO IGNORE

Time to ensure your business is ready for the changes coming down the track.

25 May 2018 looms large and businesses should be in the throes of preparation for the new General Data Protection Regulation ("GDPR"). For GCs leading on GDPR, the challenge will be translating what the rules mean for the business and whether a change in approach is required. The GDPR's explicit focus on 'accountability' and having policies and procedures to demonstrate compliance is significant, as you will be judged on how effectively you can show that the business complies and has appropriate governance measures in place.

The GDPR builds on various principles and concepts of the Data Protection Act 1998 ("DPA") as well as current data protection best practice. Many of them will not be new to businesses that presently have a strong culture of DPA compliance and they will already have a good starting point for compliance with the GDPR. However, there are some new concepts and most businesses are going to have areas which need examination and tightening up.

It can feel like there is a very large hill to climb to achieve any kind of GDPR implementation. The journey is likely to start with the audit phase and an analysis of how and why the business collects and uses personal data and how it will (or in fact whether it should) continue to do this post-GDPR.

Although there has been a lot of emphasis on the burden of the new regime, scrutinising why you are doing what you are doing can be an illuminating and beneficial process in order to iron out any poor practices that might lead to future trouble. In simple terms, principles such as 'data minimisation' and 'storage limitation' mean the business should not process more personal data than it needs and should delete data when it is no longer needed. In fact, these principles already exist under the DPA (albeit under different names), but due to the accountability principle, there will be a much more visible need to consider your data use and retention, and to have relevant policies on both. To illustrate, historically, custom and practice within an organisation may have meant that HR records were routinely sent to or were accessible by an overseas group HR function. Why this is done would need to be considered, and whether this was really necessary.

In terms of resourcing, it is likely GCs will not be working alone and will need to draw on a team across the IT, HR and marketing functions, who will have more in-depth knowledge about how personal data is processed by the business.

Taking into account data minimisation, it may be that a more limited dataset could be shared and still achieve the same business need. CRM databases may hold large amounts of personal data about customers and prospects; some of this may be quite old and not useful and therefore should be deleted. Businesses will need to have a justification for keeping old data and a process for flagging and dealing with it (whether deleting, pseudonymising or anonymising it). The need for this will become more pronounced under the GDPR because of the requirement to tell people how long you will hold their data in response to a subject access request, and to detail your retention criteria in privacy notices.

The idea of 'data protection by design and by default' means these types of considerations will need to be built into new processing operations, products and services as a matter of course. As well as minimising the amount of data that is processed, the GDPR also refers to other privacy-related measures such as pseudonymising personal data, implementing security features and ensuring that 'by default' personal data is not made accessible to persons who do not need it. It will be necessary to consider how current IT systems measure up; it may be that access to certain databases within the business could be limited or that IT systems could be re-designed for minimal privacy impact (for example, blocking websites to prevent staff misuse of the internet rather than continuously monitoring them). If you are an IT developer, you will also need to bear data protection by design and by default in mind when designing new applications that involve the processing of personal data. A privacy impact assessment will help to evaluate and mitigate any privacy issues.

Anonymisation – turning data into a form so that individuals are no longer identifiable (e.g. statistics)

Pseudonymisation – turning data into a form so that direct identifiers are removed but individuals could still be identified with additional information (the 'key') which is held separately (e.g. replacing names with code numbers)

Another key systems/process consideration is how the business will deal with information requests post-GDPR – not only subject access requests, but new erasure requests and requests for personal data in a form which can be transferred to a new provider (so called 'data portability'). It is not going to be acceptable to say that systems do not have the required functionality to sort, delete or port data, so this will need to be addressed. It will also be helpful to put in place a process to ensure requests are escalated and dealt with appropriately within the necessary timescales.

A further step will be creating workable policies and procedures for the business. This may involve (for example) a data protection policy which is rolled out to staff describing generally how the business deals with data, as well as more specific policies and procedures, for example on data retention, approaches to marketing consents, privacy impact assessments and dealing with security breaches and information requests. Depending on structure, it may be appropriate for those policies to apply on a company or group-wide level. Any policies will need to be disseminated appropriately, with training to ensure that staff collecting and using personal data are sufficiently up to speed.

In terms of resourcing, it is likely GCs will not be working alone and will need to draw on a team across the IT, HR and marketing functions, who will have more in-depth knowledge about how personal data is processed by the business. This will also assist with having a joined-up approach across those functions going forward. You may need to appoint a data protection officer ("DPO"), or you may appoint one voluntarily, outside the legal team (for example, in compliance). If this is the case, defining the separate roles and having a framework which sets out how the legal team and the DPO will work together is likely to assist. Ultimately, the DPO (if a mandatory one) will need to report to the highest level of management, but there is a potential for cross-over across the two functions, and the DPO may also need legal support.

Ultimately, there will be a lot of work to do for many businesses in the coming months to tease out these issues and figure exactly out what GDPR compliance will mean for them – since there's no arguing with the necessity of complying.

ROUND UP

- Undertake comprehensive information gathering - this will help to draw out issues and inform the business approach.
- Assess whether personal data held by the business is needed and whether you can minimise the collection and dissemination of personal data going forward.
- Think about your team – will there be a separate DPO and how will you work together?
- Put policies in place, inform staff and support with training.

Beverley Whittaker
Partner
01483 734281
beverley.whittaker@stevens-bolton.com

Ayesha Whitworth
Associate
01483 401236
ayesha.whitworth@stevens-bolton.com

M&A: MAKE SURE CYBER-SECURITY ISN'T YOUR ACHILLES HEEL

As GCs know all too well, managing an M&A process requires careful planning. However, there is an increasingly significant issue which can fall between the cracks: cyber-security. This business-critical threat should not be regarded as the preserve only of the IT department but as part and parcel of strategic and corporate risk management and therefore a fundamental part of today's M&A process.

During an M&A deal process a huge amount of sensitive data is shared in the cyber-space and infringement of this data's cyber-security could leave parties open to significant claims. In addition to any contractual obligations imposed as part of the deal, and to regulatory duties imposed under data protection legislation, both sellers and buyers (and any third party advisors) will owe: (i) an equitable duty to individuals to preserve the confidentiality of their information, and (ii) a parallel duty through the tort of negligence to keep it secure.

So how can GCs be extra-vigilant to ensure that information being collated, reviewed and negotiated is not compromised or vulnerable to cyber-attack?

Cyber policies and procedures: Review and update these at the start of every deal to ensure they reflect best practice (which is constantly evolving).

Project names: Always adopt and enforce this simple but effective security measure. Especially in email traffic, which can be voluminous and rapid, project names and party pseudonyms should be carefully and consistently used.

Confidentiality agreements: Pay careful attention to these. Ensure that they are tailored around the specific organisational and technological channels which will facilitate the deal. At a minimum, the degree of care extended to the security of data received should be that applied to your own confidential information (expect a prudent seller to carry out reverse due-diligence on your policies and procedures to check that they are actually sufficient). Ensure any obligations on you to flow-down contractual confidentiality protections to advisors or employees are strictly implemented.

Virtual datarooms: Commonplace in today's M&A landscape, these are an efficient and secure way to control and manage the flow of deal information. Being cyber data-sharing tools, virtual datarooms understandably raise lots of cyber-risk concerns in principle, but these are usually adequately addressed in practice by features such as password protection, the ability for the seller to manage individual accesses and restrictions, the option to place confidentiality watermarks on documents and the fact that due-diligence enquiries can be presented, updated and responded to all within the secure platform. GCs should therefore ensure, wherever possible, that their team members (and the seller's team) restrict the flow of data to a dataroom which supports appropriate security features and avoid using less secure channels such as email.

Anonymised data: Properly anonymised data is not subject to the requirements of the Data Protection Act 1998 (DPA) (which imposes duties on data controllers in respect of disclosing "personal data"). Prudent sellers will therefore anonymise personal data before sharing. It is recognised that in business purchase situations TUPE legislation will require the disclosure of certain personal employee information but this should still be anonymised to the fullest extent possible. Parties cannot avoid the application of the DPA. If it is still possible to identify the individual from the anonymised data sent by a seller, the buyer will itself then be 'processing' the personal data (and should arguably notify the individual whose data it is that they are doing so). Your team should therefore request and enforce anonymisation wherever possible. A request for the disclosure of personal data should only be made if the information is absolutely necessary at the relevant stage of the transaction.

From May 2018 a new set of data protection rules will replace the DPA and (amongst other things) require organisations to report personal data breaches to the regulator within 72 hours of becoming aware of them (except where the breach is unlikely to result in risk to the individual). Details of regulatory actions taken as a result of such disclosures will be publicly available. Financial penalties will also massively increase with some breaches costing businesses fines of either €20 million or 4% of global annual turnover - whichever is the greater.

In the deal planning stages GCs must therefore consider this impending change and its potential impact on timing, cost and deal-confidentiality if infringements occur during negotiations (as well as the wider, on-going implications for their (and the target's) business post-completion).

Due diligence: Data drives so much of today's business in every sector so cyber-security due diligence should be considered as part of every deal. But, as a buyer, formulating a comprehensive cyber-risk profile in respect of a target is by no means easy. GCs must appoint the right team (internal and/or external depending on the nature of the target and the types of information it holds) to ask and respond to a bespoke set of cyber-security enquiries. Full and careful analysis of the types of data held and of its cyber-security systems, processes, vulnerabilities and past-history at the due diligence stage can significantly influence negotiations and deal terms. Careful due diligence in this area will also enlighten GCs as to any required post-completion alignments to cyber policies and procedures within the group.

Cyber-security insurance: Still in its relative infancy, demand for explicit protection against cyber-breaches is increasing, particularly in response to the shocking financial and reputational impact of some recent (and very public) cases. To assist in making the UK a world centre for cyber security insurance, Lloyd's of London has recently published its "Emerging Risks Report 2017" providing insurers who write cyber coverage with realistic and plausible scenarios to help quantify cyber-risk aggregation. So now is a good time to ensure that both your business and any target businesses are appropriately protected both before and after completion.

With this variety of strategies in mind cyber-security can be carefully managed during M&A to ensure that expectations are met and all regulations complied with. As cyber-threats become more and more potent, diligence is key.

James Waddell
Partner
01483 734223
james.waddell@stevens-bolton.com

Claire Miller
PSL
01483 734250
claire.miller@stevens-bolton.com

THE ALGORITHM IS GONNA GET YOU

AI, disruption and the law.

What are the challenges associated with "the fourth industrial revolution" and what strategic impacts should GCs be considering? Assessing the likely developments now will put you in good stead. Requirements may include a greater need for flexibility and crisis management, how to cope with changes in employment law and getting to grips with new regulations (not least the new privacy requirements that are due to permeate all business). Rapidly evolving technology and its application is shaking-up society and commerce, and GCs may need to think fast about how to keep up.

Flexibility in a crisis

The current effect of modern technology on society is seismic. The rise of social media is widely acknowledged to be a significant contributing factor to disruptive geopolitical events, from unpredictable election results to the so called 'Arab spring'. Some experts predict further geopolitical instability caused by technological developments. Indeed, some believe relatively-speaking that we are only in the foothills of change and the real effects are yet to be experienced.

The application of modern technology to business is characterised by very high levels of competence, context, efficiency and financial gain, coupled with an exponential growth in market penetration... and the occasional, uncontrolled catastrophic failure! We have the accelerating risk of cyber threat, like the recent ransomware attacks on the NHS, and systemic failures caused by greater automation and autonomisation. Flash crashes caused by high frequency

trading are a good example of this. The speed with which computer systems can operate clearly brings benefits, but the risk of corresponding issues is a growing burden.

Accordingly, legal teams will have to operate more flexibly and nimbly on a global basis. An ability to effectively manage major crises will be more important than ever and lawyers are likely to have a key role in the analysis of all risk areas. GCs will need to assess whether they have the right personnel with the right skills to manage the risk, be it internal, external or both.

The ability to defend or attack increasingly polarised market positions

Without a doubt, we are seeing a trend generally towards increasingly concentrated markets. For example a recent OECD report states: "One factor is that the state of competition in major economies, like the United States, is worrisome, with evidence of increasing concentration and greater profits flowing into fewer hands."

This tendency towards concentration, and the benefits of economies of scale, might be exacerbated by increased reliance on 'big data' and networks. So called 'network effects', where the size of the network increases its value, leading to exponential growth, might mean repeated patterns of initial competition for a market followed by the domination of one market leader. Google's share of the search engine market is testament to this.

We expect more stratified markets, with more clearly defined winners and losers. In-house counsel representing the winners must be prepared to defend their position, and must expect sustained legal attacks from competitors and regulators. Lawyers representing challenger businesses must be adept at using the law and other means, like government lobbying, to challenge incumbents with very significant market power.

Adaptability in employment law and the nature of work for GCs

It is fairly safe to assume that significant changes to the workforce are coming. The Government Office for Science's report entitled "Artificial intelligence: opportunities and implications for the future of decision making" reports that 10-35% of jobs will be affected by automation over the next 10 to 20 years. But the actual implications of this are unclear: a US survey of experts suggested that 48% believe there will be an overall decline in the level of employment, and 52% believe that there will be an increase. Of some comfort to professionals is that the number of skilled jobs is expected to rise, with demand for skilled jobs expected to exceed supply by 2022. It is also anticipated that workers will need to find areas where human skills, such as empathy or creativity, are more in demand.

The application of modern technology is characterised by very high levels of competence……and the occasional uncontrolled catastrophic failure!

Employment issues for businesses will continue to increase, at least in the short to medium term, with significant redundancies and reskilling. As well as managing an increased employment law workload for the business, given organisational changes, there will be personal demands placed on the GC, to grapple with and learn new areas, and to work with new technology. With computers handling more routine tasks GCs may find themselves managing smaller, nimbler teams, and there may be greater challenges in developing teams and keeping them motivated.

Getting to grips with new regulations

It's fair to assume that the regulatory landscape will continue to evolve at pace. There are significant challenges for governments and regulators, in seeking to keep up with new developments. For example, in relation to autonomous vehicles, governments across the world are grappling with regulatory approaches. The UK has written a number of position papers on autonomous vehicles, and has tabled a new bill regarding liability, while the US Department of Transport is considering a wider array of regulations, around premarket testing and ongoing supervision of vehicle systems. There is an increased interest in the analysis and regulation of algorithms and code. Almost all businesses are likely to be affected one way or another with new regulatory challenges.

For in-house counsel, identifying and keeping in touch with regulatory developments in your particular area is crucial. There will come a point where AI and deep learning may be able to help with this, but in the meantime there is unlikely to be a let up in the ever-increasing regulations that apply to businesses.

Data privacy expertise

The use of big data and machine learning means that all businesses are likely to be reliant on customer data, from the relatively mundane to the highly sensitive. This, and the related introduction of new laws and more prevalent and draconian enforcement, means in-house lawyers must become data privacy experts.

There is a considerable change occurring all around us, with the advent of AI. While this is undoubtedly daunting and challenging, it is also unavoidable, and as such we need to grapple with it, including the tactics detailed above. As Abraham Lincoln said, "You cannot escape the responsibility of tomorrow by evading it today".

Gary Parnell
Partner
01483 734269
gary.parnell@stevens-bolton.com

LITIGATION V ARBITRATION

Which is better when it comes to cross-border disputes?

"Preparation is the key to success": so said Alexander Graham Bell and never has this adage been more true than when dealing with cross-border disputes, which are best assessed and planned for long before the dispute arises!

In any international trade, the parties are immediately faced with choices, risks and consequences that can greatly affect the handling and outcome of any disputes that arise. For that reason, it is particularly important to consider in advance the key commercial risks that a proposed transaction carries and to give thought to how best to protect the business from them. In the face of Brexit, this is essential now more than ever before.

Of course, before doing business in any new jurisdiction, it is vital to have given some thought to local law. From a litigation perspective, the courts in each jurisdiction have their own processes and idiosyncrasies that can be terribly frustrating (and costly) if not properly understood and managed. Fundamental issues, such as the right to damages or the recovery of legal costs, can vary significantly.

For this reason, parties are often tempted to contract under the laws of third party countries, in order to ensure that the contract is robust and can be enforced under sensible laws in a sensible set of courts. However, that is only part of the picture, because ultimately a distinction must be drawn between obtaining a judgment, which is after all just a piece of paper with words on it, and actually achieving the objective of the litigation, be it financial compensation, the return of a valuable asset or something else.

English law has long been popular for international contracts. The English legal system and courts are seen as sensible, stable and objective in their approach. They can be expensive and slow, but tend to reach the right outcome in most cases. English law judgments are widely enforceable, due to our current membership of the EU, our former commonwealth and various other treaties and agreements. English courts also generally work in the English language, which is very widely used in commerce across the globe. Of course, some of this might change post-Brexit, but that remains to be seen.

"start from the commercial risk and anticipated disputes and work backwards to determine the best choice of dispute resolution forum and process"

However, if the contract counter-party is based in a jurisdiction that will not readily enforce an English or other neutral law judgment, and that is the jurisdiction in which the contract might be performed, then all of that sensible legal analysis could be a waste of time!

One common means by which to meet a set of competing issues on jurisdictional choices is to opt for arbitration. This is a very common choice in international commerce. Arbitration is neutral as regards jurisdiction. It will apply the laws of the contract in determining a binding outcome, but is not court-based and can be seated anywhere in the world. It is often more private than court proceedings and in some circumstances the choice of arbitrator(s) can allow the parties to select someone with real market knowledge, which can help ensure a proper understanding of the commercial issues. However, arbitration can be expensive, as the tribunal is privately funded, and there are circumstances in which arbitration can be cumbersome and formulaic - for example where urgent injunctive relief is required. However, it is upon enforcement that the balance tends to shift firmly in favour of international arbitration over litigation, at least in theory. There are 157 signatories to the New York Convention, meaning that a properly constituted and decided arbitration award should be directly enforceable in each of those states. That is far wider than any Court's decision. This can be particularly useful where an arbitration award might require enforcement in more than one jurisdiction. However, none of this is ever perfect and just because a state has signed the New York Convention does not mean that a particular arbitration award will be easily enforced in a particularly difficult jurisdiction. However good the contract or however watertight an award, problems can still be encountered at a local level upon enforcement.

Where contracts might require urgent injunctive action, such as the need to recover or freeze a valuable asset on short notice, parties will often agree a split clause that requires arbitration for the resolution of substantive disputes while affording the option to one or more parties to invoke the jurisdiction of courts to protect its asset. These can be very useful to one or more parties, but it is really important to think about the particular jurisdictions involved, as some will not enforce them in all circumstances (such as Russia and France).

The enforcement of arbitral awards will likely be unaffected by Brexit. However, the impact on court proceedings between the UK and EU states is a matter that will require careful negotiation. For this reason, contracts including multiple European states might benefit from arbitration provisions while the uncertainties of the post-Brexit world remain unresolved. This all contributes to the choices counsel face, especially when dealing with cross-border disputes – regarding litigation and arbitration, and their respective merits.

LITIGATE OR ARBITRATE: THE KEY QUESTIONS

1. In which jurisdictions might disputes arise, and where might enforcement take place? What are the rules for enforceability in those jurisdictions? What are the court systems like?
2. What sort of disputes might arise - for example the urgent recovery of an asset or other injunctive relief? What are the commercial objectives that might need to be achieved?
3. Is confidentiality a key issue? Or cost/timing?

ISSUE	LITIGATE	ARBITRATE
Enforceability	Where will judgment be obtained and can that be enforced locally when needed?	Will the state where enforcement will be required enforce an arbitration award?
Urgent relief	Will the Courts where relief is required grant or enforce an injunction?	Is this a key element of the claim? If so, litigation might suit better.
Confidentiality	In most jurisdictions, court proceedings are public.	Arbitration is mostly held in private and is confidential.
Multi-jurisdictional dispute	May require proceedings in a number of jurisdictions.	A single award might be directly enforceable in a number of jurisdictions.
Can't decide?	Consider split jurisdiction clause...	...But beware attitude of local courts.

Richard Mumford
Partner
01483 734245
richard.mumford@stevens-bolton.com

Michael Frisby
Partner
01483 734244
michael.frisby@stevens-bolton.com

Forthcoming Stevens & Bolton events

12 October
Entrepreneur Forum 2017
Bridging the scale-up in Brexit Britain – Guildford

12 October
HR Directors Breakfast Club
The new GDPR and Employment Update – London

7 November
In-house Lawyer Legal Update – Guildford

23 November
Immigration Seminar – London

For further information about our events programme, please visit www.stevens-bolton.com

Get involved

Follow us on Twitter: @stevens_bolton or find us on LinkedIn: Stevens & Bolton LLP

We created this magazine with the aim of developing a valuable resource dedicated to GCs, exploring the topics that might impact you the most. We would welcome feedback, so please do get in touch if you have any comments or ideas for topics you would like us to explore in future issues.

Please contact Laura Reynolds, Brand & Communications Manager,
on 01483 401244 or laura.reynolds@stevens-bolton.com

STEVENS&BOLTON

Wey House, Farnham Road, Guildford, Surrey GU1 4YD

Phone: +44 (0)1483 302264
Fax: +44 (0)1483 302254
www.stevens-bolton.com