Employment Law Briefing

Volume 12 | Summer 2016

Brexit — Keep Calm and Carry On

By Dan Peyton & Sarah Thompson

The Brexit referendum elicited strong feelings amongst "Leavers" and "Remainers", and will likely continue to do so. In the UK it is generally not as common for co-workers to discuss their political views as it is in, say, the U.S. However, the referendum certainly prompted such discussions both in the workplace and on social media. This creates some potential employment issues for employers to be alive to.

1. The line between legitimate political expression on the one hand and expressing views that are unacceptable can be crossed very quickly.

With feelings running high and discussions involving sensitive topics (such as immigration and people's reasons for voting one way or another) there is potential for political discussion to degenerate into bullying, harassment and, potentially, discrimination. For example, the suggestion that those who voted for Brexit did so for racist reasons has the potential to cause grave offence and could constitute bullying and harassment depending on the circumstances. Similarly, discussions about "sending home" non-UK nationals following the vote could constitute unlawful discrimination.

Employers should not interfere with employees' freedom to discuss political issues in the workplace but need to be aware of these potential problems and deal with them sensitively but quickly and firmly, intervening where necessary.

2. It is widely anticipated that there will be at least some changes to the immigration rules regarding EU nationals entering or residing in the UK once Brexit occurs.

Employers who try to pre-empt the future of EU citizens' immigration rights could find themselves falling foul of discrimination law. Decisions regarding recruitment, promotion and/or termination should not be based on an individual's nationality; a "protected characteristic" under the Equality Act 2010. The Equality Act applies to job applicants as well as employees (used in the wider sense). Therefore, an employer who rejects a candidate because they are an EU citizen (due to potential, as yet unknown, future restrictions on EU citizens rights to work in the UK post-Brexit) would likely be unlawful. Similarly, if redundancies are contemplated, deciding to make an individual who is not a UK citizen redundant on the basis that there may be future immigration restrictions would also risk breaching the Equality Act. Whilst Brexit is at the front of our minds, businesses should be conscious not to base employment decisions on potential future immigration changes.

3. On the other side of the coin, employers may have employees who feel unsettled or uncertain as a result of the vote for Brexit.

For example EU nationals from other EU member states. It is tempting to offer comfort to individuals in this position, particularly highly valued employees, who may have fears regarding whether they will be permitted to remain in the UK once the UK's terms for exiting the EU are agreed. However, employers should be careful not to make commitments which may be difficult or impossible to deliver and which could be construed as contractual promises or, at the very least, inducements for employees to stay that may prove to have been misleading.

McGuireWoods London LLP
Employment Team Members:

Dan Peyton, Partner
+44 20 7632 1667
dpeyton@mcguirewoods.com

Sarah Thompson, Associate
+44 20 7632 1693
sthompson2@mcguirewoods.com

Andrea Ward, Senior Associate
+44 20 7632 1697
award@mcguirewoods.com

McGuireWoods London LLP
11 Pilgrim Street
London EC4V 6RN
United Kingdom
DX 249 London/Chancery Lane

Brexit Checklist – Data Protection

By Sarah Thompson

Whilst we wait to see what the Brexit result will mean for the UK's data protection regime, it is important to recognise that the result will not change anything immediately. The exact nature of the post-Brexit UK-EU relationship will influence any UK data protection reform, and it is highly likely that the UK will continue to be heavily influenced by EU laws. Indeed, the Information Commissioner's Office (ICO) (the UK's data protection authority) has emphasised this and also highlighted that the UK's Data Protection Act 1998 (DPA) remains the law for the time being, irrespective of the referendum result. So what should businesses be doing in the meantime?

1. Prepare for the GDPR and changes to UK data protection laws

Data controllers established in the UK and processing personal data in the context of that establishment are currently subject to the DPA. Once the EU's General Data Protection Regulation (GDPR) comes into effect on 25 May 2018, the UK will still be a member of the EU, so the GDPR will automatically replace the DPA. UK companies will then need to comply with the new regime until Brexit occurs. Following that, the GDPR will fall away but we do not yet know what form any replacement legislation will take. If the UK wants to continue trading with other EU member states, it will likely need to adopt legislation similar to the GDPR. With this in mind, businesses should continue with their GDPR compliance preparations.

a. *What steps are being taken to prepare for the GDPR?*

b. *Document what personal data the business holds, where the data came from and with whom data is shared.*

c. *Review current privacy notices and determine what changes are required.*

d. *Check current data protection procedures and determine what changes are required.*

e. *Monitor the ICO's guidance on Brexit and the GDPR, and update organisational plans as and when new guidance is released.*

2. If targeting EU citizens, continue complying with the GDPR

The GDPR will apply not only to businesses established in the EU, but also to businesses outside the EU that process personal data of EU citizens, either by offering services or goods or from monitoring behavior. Therefore, following Brexit, the GDPR will still apply to UK-based businesses trading with the EU or targeting EU citizens. Such businesses therefore should continue their GDPR compliance efforts.

a. *Identify those activities that involve processing of personal data of citizens in other EU member states.*

b. *Establish and commence a compliance plan for the GDPR.*

3. Consider where personal data is processed and transferred

EU data protection laws prohibit transfers of personal data to countries outside the European Economic Area (EEA), unless they have been recognised as providing "adequate protection" to personal data. Companies need

to consider whether they receive data in the UK from global regions which are currently compliant based on the UK being within the EU or EEA. If the UK is not classified as "adequate" post-Brexit, UK companies receiving data from the EEA will need to re-think their data protection compliance strategy and put in place adequate safeguards, such as Model Clauses or Binding Corporate Rules.

In addition, the converse (transfers outside the UK) may also be an issue so companies should consider whether they send personal data from the UK and what compliance measures they may need to put in place. Following Brexit, the EU-U.S. Privacy Shield will not cover transfers from the UK to the U.S. However, the ICO could approve the Privacy Shield as an adequate means of data transfer from the UK to the U.S., or it could establish a similar framework (e.g., one like the U.S.-Swiss Safe Harbor framework).

a. *Map out the organisations data flows.*
b. *Where is personal data collected?*
c. *Where is personal data stored? Where are systems or servers located?*
d. *Is personal data received in the UK from other EU member states?*
e. *Is personal data transferred outside the UK, and if so, where? Do global operations access personal data housed in the UK?*
f. *Are Model Clauses or Binding Corporate Rules currently in place? If so, what data transfers do they cover?*

4. Consider third-party service providers

Again, it is likely that if the business uses third-party service providers located outside the UK, personal data will be transferred outside the jurisdiction and be subject to the international data transfer principle.

a. *Does the business engage third-party service providers?*
b. *Where are those service providers located?*
c. *Is personal data transferred to those service provides?*
d. *What documentation is currently in place with third-party service providers?*

5. Determine where the organisation's main EU establishment will be

Some GDPR provisions are dependent on the "main establishment" of a business being in the EU. Once the UK leaves the EU, a company with UK-based headquarters will no longer count as the main establishment under the GDPR following Brexit. This will affect a company's lead data protection supervisory authority under GDPR for the purpose of enforcement and other reasons such as approval of Binding Corporate Rules.

a. *Where is the company's main EU establishment?*
b. *If the main establishment is in the UK, where will the company's main establishment be once the UK leaves the EU?*
c. *Is the business in the process of obtaining Binding Corporate Rules? If so, through which supervisory authority?*

It is hard to predict at the moment precisely the timing and scope of legal changes to the UK's data protection regime resulting from Brexit. We will continue to monitor developments closely and keep you fully informed as the post-Brexit process unfolds.

Related Event:

SAVE THE DATE

McGuireWoods Annual European Data Protection and Security Conference

September 27, 2016
London

Learn more about data protection laws in light of Brexit. The conference is designed for inhouse counsel, risk managers, security officers, regulatory and compliance officers, directors, financial officers, information officers, human resources officers and managers of corporations with cross-border operations. A full agenda is under development, but topics and speakers from last year's event can be viewed here.

Click here to ensure you receive an invitation to our 2016 conference.

Brexit Checklist — Employment Law

By Dan Peyton

Employment law is another area where change is likely, given the extent to which current UK legislation and English case law is driven by the EU. Although the precise nature and magnitude of change is difficult to predict at present, there are some steps that employers can take at this stage to ensure that they identify areas of potential risk and position themselves to react in the way that best suits their businesses as and when change comes.

1. Prepare for possible changes to free movement of workers

We do not yet know what, if any, changes will be made to the free movement of workers. However, given that this was a cornerstone of the Leave campaign, it is likely that there will be changes in this area. Employers should prepare for possible changes by establishing the number and roles of affected employees so that as and when new rules are introduced, the nature and scale of the issue is already identified, can be monitored, and solutions can be found.

a. *Do you have employees who are nationals of EU member states?*
b. *Do you have UK nationals living and working in other EU member states?*
c. *How many, where are they and what are their roles?*
d. *Do you have roles or functions that may need to be relocated?*

2. Review contracts of employment and policies for EU-specific or -driven terms

Many contractual terms and employment policies and practices are currently driven by the need to comply with EU-originated law. Employers should prepare for possible changes in these areas so that they are ready to respond in the way best suited to their businesses. As a first step, ensure that the business is aware of terms and conditions and policy provisions that are EU-originated and vulnerable to change including:

a. *Working time*
b. *Holiday entitlement*
c. *Leave and accrued rights (e.g. holiday during sickness and maternity leave)*
d. *Commission, overtime and holiday pay*
e. *Data protection issues*

f. *Bonus caps pursuant to the Capital Requirements Directive*
g. *Collective redundancy consultation*
h. *Jurisdiction and choice of law*

3. Consider agency worker roles, terms and conditions

Agency worker protections emanate from the EU Agency Workers Directive which may be repealed or reformed in the interests of maintaining flexibility in the workforce. Employers should be ready to respond or take advantage of any changes if in the interests of their businesses.

a. *Do you have agency workers?*
b. *Are there roles that would be suitable for agency workers if the regulations were not in force?*
c. *How many?*
d. *Which roles?*
e. *What are the actual or preferred terms and conditions for these workers?*

4. Review collective consultation arrangements

Works councils, transnational works councils, consultation obligations on redundancy and TUPE transfers are all EU-originated laws and so change to these laws is possible. Employers should consider what mechanisms are currently in place as regards UK employees and the extent to which those mechanisms are desirable in the context of their business.

a. *What collective consultation arrangements are in place?*
b. *Which are solely domestic and which cover more than one jurisdiction?*
c. *Which are effective and suit the needs of the business and which are not?*

5. Protect business assets

As in the case of any commercial disputes, employers need to keep under review whether there are any changes to jurisdiction and choice of law rules, currently harmonised across the EU. If there are changes to the applicability of these rules, this may impact the ability of employers to protect business assets through, for example, the enforcement of post-termination restrictive covenants.

a. *Where are your business assets and the employees with access to them located?*
b. *In which jurisdictions could they be at risk?*
c. *Do you have contractual and practical protections in place?*
d. *Do those protections deal adequately with the potential need for cross-border enforcement?*