Impact of Brexit on General Data Protection Regulation

The data protection laws in the United Kingdom (‘UK’) are currently governed by the General Data Protection Regulation ('GDPR'), which came into effect across all European Union (‘EU’) member states *(including the UK)* on May 25, 2018; and serves to create a harmonized legal framework regulating the way in which personal data is collected, processed, archived and shared throughout the EU.

UK's prospective relationship with the EU post Brexit
If the UK withdraws from the EU, it may be granted membership to the European Economic Area ('EEA') trade group, which adopted GDPR in July 2018 and accordingly, personal data in Britain would continue to be governed by GDPR. However, as one of the main drivers of Brexit was to achieve independence from the rules and regulations of the EU and the EEA; it appears unlikely that the UK will join the EEA.

If the UK joins the European Free Trade Association ('EFTA'), which is relatively more relaxed from a legislative standpoint, then its citizens will not be covered by GDPR. This is consistent with the relationship that Switzerland has with the rest of the EEA.

Data protection after a 'No-Deal Brexit'
If the UK leaves the EU with no withdrawal agreement in place, then GDPR will no longer be applicable effective from the date it leaves the EU.

Data protection if an 'Exit Deal' is signed with the EU
While there is much speculation regarding the final consensus between the UK and the EU over Brexit, the UK's current proposed draft expressly states the ultimate goals for personal data protection. The draft withdrawal agreement sets forth a transition period through December 31, 2020, where EU laws *(including GDPR)* will continue to apply to personal data that is processed before or during the transition period. However, as the UK is committed to maintaining an equivalent data protection regime, a UK version of GDPR will come into force following the departure date *(exit-day)*.

This will be achieved through the European Union (Withdrawal) Act, 2018, which incorporates the body of EU law *(including GDPR)* as it exists on exit-day, into UK's law thereafter *(UK GDPR).* A statutory instrument will apply necessary changes to GDPR to make it relevant to the UK following its departure from the EU - for example, to remove references to cross-outskirt data exchange moves with other member states and contribution in EU wide-establishments such as the European Data Protection Board (‘EDPB’). These changes can be found within the **Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.** It follows that the Data Protection Act, 2018 will remain in place alongside GDPR as supplementary legislation and the Privacy and Electronic Communications (EC Directive) Regulations 2003 will remain intact, although references to GDPR will automatically be converted into references to the UK GDPR.

GDPR imposes restrictions on the transfer of personal data to a ‘third country’. The UK Government has stipulated that following Brexit it does not intend to apply these restrictions on transfers of personal data from the UK to the European Economic Area. Consequently, UK-based organizations will continue to be able to send personal data to organizations in the EEA. UK-based organizations will also be able to continue to rely on the EU/US Privacy Shield scheme to send personal data to registered entities in the US, but only where the US entity has modified its privacy notice to apply its coverage specifically to UK transfers. These are intended to be impermanent measures and it is proposed that the UK will carry out its own adequacy tests *(inclusive of EU Member States)*.

Nevertheless, the EU has not proposed similar changes with respect to transfers to the UK. The transfer of personal data from the EEA to the UK will be limited once Brexit takes place successfully. This will have a major impact on any organization that routinely transfers personal data from the EU to the UK *(including UK-based organizations providing services to customers in the EU)*.

If an organisation has processing activities in both the EU and UK or is targeting customers or monitoring individuals in the EU from the UK *(or vice versa)*, it is likely that the organisation will be subject to regulatory responsibilities under both the EU and UK versions of GDPR following Brexit. This is due to the extraterritorial scope of GDPR in Article 3. Depending on the circumstances, this may result in additional compliance requirements relating to the following.

• Appointment of a distinct data protection office ('DPO') for both the UK and EU;
• Appointment of a new lead supervisory authority in the EU as well as registering with the Information Commissioner's Office ('ICO') for processing activities in the UK;
• Appointment of a local agent in the EU/UK, where you are processing data from outside the jurisdiction; &
• Management of probable exposure to sanctions/fines under both the EU and UK regulatory enforcement regime, i.e. risk of double jeopardy for any transgression.

Set below are some possible scenarios for GDPR after Brexit, depending on the role of the business in the data flow.

Scenario 1 | Controllers in the UK, providing services for UK people and entities and sharing no personal data with organizations outside the UK - the controllers defined by scenario 1 are the least affected by GDPR after Brexit.

Scenario 2 | Controllers in the UK, providing services for the UK but involved with processors in the EU *(or anywhere else outside the UK)* - the processors outside the UK will still be compliant with GDPR and there is nothing that hinders these UK controllers from continuing to use their services.

Scenario 3 | Controllers in the UK, providing services for people and business entities in the EU - obtaining more clients in the EU market will be difficult. It will be harder to compete with EU controllers who do not have post-Brexit ambiguity to sort through.

Scenario 4 | Processors in the UK, acting on behalf of controllers or processors in the EU *(or UK and EU)* - there is the risk that some of your business partners will decline to resign. Continuing to do business with them in the absence of a thorough assessment of proper documentation work is another risk of grave threat.

Scenario 5 | Processors in the UK, acting on behalf of controllers or processors in the UK.
For processors in the UK working only with data of people within the UK *(and for controllers in the UK)*, the same applies as in Scenario 1 - simply put, there is no essential change.

Although the EDPB, Information Commissioner's Office, and the UK Government [Department for Digital, Culture, Media and Sport ('DCMS')] have all issued guidance on handling the ramifications of Brexit on data protection, it is advisable for all stakeholders to maintain their alertness on the same.

Conclusion
As of now, the UK and the EU do not seem close to have accepted a mutually agreed withdrawal agreement. Accordingly, GDPR's ultimate application for the UK remains uncertain at this stage. Considering the close association between UK companies and other EU member states, there are

strong economic and operational reasons to maintain and safeguard the UK privacy laws in conformity with GDPR post-Brexit.

Please do not hesitate to contact any of our GDPR experts *(whose coordinates are given below)* for any queries you may have or assistance that you may require.

Lalit Sharma | Associate Director | lalit.sharma@mgcglobal.co.in
Gautham Desai | Manager | gautham.desai@mgcglobal.co.in