Howden Group Holdings

Data Transfers – A Post Brexit Data Protection Update for Clients and Partners (January 2021)

1. Post Brexit summary

On 31 December 2020 the Brexit transition period ended, and the provisions of the UK-EU Trade and Co-operation Agreement took effect. Chapter 7 of the Final Provisions of the Co-operation Agreement provides for the continued free flow of personal data from the EU/EEA states to the UK until an adequacy assessment is completed, and for this assessment to take no longer than 6 months.

So:

- For the moment, the UK is not termed a "third country" under EU data protection law, and so personal data can flow freely from the EU/EEA to the UK.
- The UK will amend the EU GDPR into UK law via the European Union (Withdrawal) Act 2018 and it will then become the UK GDPR.
- The UK GDPR will be amended by secondary legislation, The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 to make it reflect UK law, and replace references to the EU with the UK.

What should I be doing?

In the next few months, it is suggested that you undertake the following activities:

1. Make sure you understand where your data subjects are located and where their personal data is stored.
2. Undertake an assessment to determine whether your business will be subject to the UK GDPR and/or the EU GDPR.
3. Include a data export mechanism in contracts with third parties for exporting data from the UK to non-EEA countries and to countries not deemed adequate by the European Commission. The data export mechanism, such as the Standard Contractual Clauses (SCC's), will also require additional due diligence in relation to the importing company and the wider data protection laws of the country in which they operate.
4. UK driven contracts will need to be updated to reflect the UK legislation that applies to the processing of personal data.
5. Amend breach notification procedures. If UK law applies, then, where required, personal data breaches would have to be reported to the Information Commissioner's Office ("ICO"). Where organisations are operating across EU, and are affected by the personal data breach, then breach reports would also have to be made to the EU lead authority, in addition to the ICO.
6. For UK businesses, the ICO will no longer be able to serve as a lead authority for the approval of Binding Corporate Rules ("BCRs") across EU member states. Where the ICO is the lead authority for existing BCRs this would need to be transferred to an EU regulator. Approval of BCRs will be required by both the ICO and an EU supervisory authority where both UK and EU

law apply. However, the ICO will not be able to approve BCRs for six months, or until a decision on adequacy has been made.

7. Consider whether you need to appoint a UK and/or EU representative. Where an organisation based outside of the EU currently appoints a representative within the EU, it would require a representative within both the UK and within the EU where both UK and EU law apply.

8. Amend any existing One-Stop-Shop arrangements. Controllers and processors that carry out processing which impacts individuals in more than one EU or EEA state may only need to deal with a single EEA data protection regulatory authority. In the event that the UK does not receive an adequacy decision and where processing in the UK is not likely to substantially affect individuals in any other EU or EEA state, then the One-Stop-Shop and lead authority arrangements will cease to apply, and an organisation will deal only with the ICO. Where you are subject to both UK and EU data protection laws in the processing of personal data you will have to deal with both the ICO and the lead supervisory authority within the EU/EEA where you have a lead authority.

9. Amend UK driven internal policies and external notices to refer to UK GDPR (and/or EU GDPR, as appropriate).

If there is no adequacy decision in the next 4-6 months, then organisations will need to ensure the following:

a) Data exports from the EU to the UK will require a data export solution as per current rules under GDPR for personal data exports to third countries, such as the SCC's or a derogation.

b) The privacy notices of EU exporters need to provide information on this transfer and the mechanism for the transfer as per existing rules under the GDPR.

2. Schrems II Court Ruling

On 16 July 2020 the Court of Justice of the EU (CJEU) ruled that the EU-US Privacy Shield framework (which enabled compliant data transfers from the EU to the US), was no longer valid and could not be used going forward.

The Court also ruled that the European Commission endorsed Standard Contractual Clauses (SCC's), which are the main mechanism for enabling the compliant transfers of personal data from within the EU to jurisdictions outside of the EU were valid. However, in its judgement the Courts emphasised the need for more robust due diligence when sharing data outside of the EU, and that organisations need to assess the privacy regime of the recipient jurisdiction, especially in relation to data access by the security services, and implement additional safeguards if the SCC's do not ensure adequate protection.

As such, simply implementing the SCC's is not enough (as it once was), and data exporting organisations should undertake more detailed assessments of the recipient's jurisdiction and act accordingly.

What should I be doing?

We are still waiting formalised guidance on this matter from the European Data Protection Board (EDPB) however, recently released draft guidance has given us an indication as to the expected requirements. In the interim there are actions businesses can consider to help minimise their compliance risks:

1. Identify where Privacy Shield has been relied upon as the basis for transfers to the US and put in place SCCs.

2. Identify other data flows, both intra-group and externally, and the mechanisms used to ensure compliance in case these need to be reviewed, amended or replaced.

3. Stay alert for guidance in your jurisdiction. Some national data protection authorities (DPAs) seem to be taking a softer approach than others, but a more harmonised approach is likely to emerge as the DPAs work within the EDPB.

4. Additional contractual clauses could be beneficial as additional safeguards, especially in relation to requests from public authorities.

5. Consider if any other measures may assist including, further limiting the volume and/or sensitivity of data transferred to 'third' countries and try to keeping data within the EU where possible to do so.

6. Include contractual provisions allowing for a change of the transfer mechanism as soon as a better one becomes available – there is the prospect, in the medium-term, of an updated Privacy Shield emerging in the context of EU-US data transfers, for instance, as the US Department of Commerce has alluded to.

7. Explore additional technical methods for minimising the risks to individuals, without effecting the purpose of the processing for the data exporter.

8. Consider if any of the derogations provided for in the GDPR in relation to data transfers are relevant or practical for any specific transfers. The derogations should not be used for regularly transferring personal data.

9. Consider whether increased transparency as to the potential for public authority access in the third country would be helpful