onside law
sport-fashion-media

UK DATA PROTECTION LANDSCAPE – 2021 AND BEYOND

The UK formally left the EU on 31 January 2020, but we will not be feeling the full effects until 1 January 2021, when the current Brexit transition period expires. Given the high standards imposed by the General Data Protection Regulation (**GDPR**) when it came into force in May 2018 (as supplemented by the Data Protection Act 2018 (**DPA**)), the UK will thankfully be doing little to deviate from these standards going forward. While there will be certain technical changes to the underlying laws and a few more substantive changes (in each case as summarised in this note), the legal and practical obligations that organisations face will be largely unchanged in practice. On this basis, if your organisation is already compliant with existing data protection laws, the transition into next year and the post-Brexit world, should not prove too onerous.

HOW ARE OUR DATA PROTECTION LAWS CHANGING FROM 1 JANUARY 2021?

1) CONVERSION OF EU LAWS INTO DOMESTIC LAW:

The European Union (Withdrawal) Act 2018 will convert **GDPR** and the **Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)** into UK law.

The converted GDPR will be known as **UK GDPR** and in practical terms, its provisions will essentially mirror the GDPR.

2) CONTINUATION OF EXISTING LAWS:

The current EU **GDPR** will continue to apply to UK based businesses which:

a. Also have an establishment in the European Economic Area (**EEA**) (e.g. a branch or office in an EEA state); and/or

b. Offer goods/services to, or monitor the behaviour of, individuals in the EEA

The DPA will continue to apply to all UK businesses and supplement the UK GDPR in the same manner it has done for the GDPR to date.

3) AMENDMENTS TO THESE CONVERTED AND RETAINED LAWS:

The **Data Protection, Privacy and Electronic Communications (Amendments etc)(EU Exit) Regulations 2019** will make various amendments to the UK GDPR, PECR and the DPA, which other than those mentioned below, are of a minor/technical nature to account for the fact that the UK will no longer be in the EU.

Where does this get us?

From next year, you will need to comply with:

- **UK GDPR**
- **PECR**
- **DPA**
- **GDPR** (*if you fall within the extra-territorial scope referred to in box 2).*

WHAT ARE THE MAIN CHANGES IN PRACTICE?

1. *International transfers of data*

There are two key points affecting which rules will apply for international data transfers:

a. Which countries will the data physically be starting from and ending in? *Note: the location of the servers housing the data is key, rather than where the relevant entities are based.*

b. Whose personal data is being transferred? Note: *regardless of where the data is transferring from, where the transferring data relates to individuals in the EEA (**EEA Data**), the GDPR (and not the UK GDPR or other foreign data protection laws) will apply to that transfer (e.g. if an English football club shares the personal data of its EEA-based fans with a commercial partner in Thailand for marketing purposes, the GDPR would apply to that transfer).*

If the UK receives an adequacy decision from the EU Commission (meaning that the UK's data protection standards are deemed adequate under GDPR, without further safeguards being required for the storing and use of data in the UK), the UK will be treated for data transfer purposes as though it were still in the EU – i.e. the position for international data transfers would be the same as it is currently. However, no adequacy decision has so far been made in relation to the UK (although it may yet form part of a deal with the EU). In the absence of an adequacy decision, the UK will constitute a "third country" for GDPR purposes when the transition period expires, which will have the following implications on the transfers of personal data between businesses, into and out of, the UK:

- *Transfers from the EEA to the UK*

These will constitute "restricted transfers" under GDPR (irrespective of whether the data relates to individuals within the EEA) and on such basis, will operate in the same way as a transfer would from the UK to any non-EEA country (see

below). Certain transfers will be subject to exceptions, but only where they are occasional, non-repetitive and meet one of a short list of conditions (e.g. the relevant individual has consented, the transfer is required to perform a contract with the individual or the transfer is to protect the vital interests of the individual etc). For example, if an athlete suffered a life-threatening injury or illness while competing in the EEA and local medics needed to seek the urgent advice of their UK doctor, it is likely that an exception would permit this transfer.

If an exception does not apply, it will be necessary to implement "appropriate safeguards" in connection with the transfer. In many cases, the most practical means of achieving this will be for the data importer and data exporter to enter the standard contractual clauses prescribed by GDPR, although other measures that adequately safeguard the relevant data may also be appropriate (including "binding corporate rules" for intra-group transfers).

- *Transfers from the UK outside of the EEA*

The UK will be publishing a list of "adequate" territories to which transfers will be permitted without additional safeguards – this is likely to align with the EU Commission's adequacy decision list. Where the transfer is going to a non-EEA country which is not on the UK's adequacy list, the transfer will be subject to the same transfer restrictions under UK GDPR as are currently in place under GDPR (and which in principle, are those outlined in the above section for EEA to UK transfers). Therefore, organisations should already be familiar with these and have appropriate safeguards in place for all existing non-EEA transfers.

It is worth bearing in mind that the invalidation of the US Privacy Shield regime earlier in the year (via the European case known colloquially as Schrems II) means that additional safeguards will always be required for transfers to the US.

- *Transfers from a non-EEA country to the UK*

Entities transferring data to the UK from non-EEA countries will need to establish how they can comply with the local law requirements of the originating country when they transfer data to the UK (e.g. an Australian professional cricket team temporarily releasing one of its contracted players to play for an English County team would need to consider what steps are required under Australian data protection laws in relation to the transfer of that player's personal data to the English team).

- *Transfers from the UK to the EEA*

These will be unaffected as the EEA will still be viewed as having suitably high data protection standards for the processing of personal data, without the need for additional transfer safeguards.

2. *European Representative*

If your organisation is UK based with no EEA office or branch, but will continue offering goods/services to EEA individuals or will monitor their behaviour, you might need to appoint a European Representative (on the basis that you are still required to comply with GDPR). The representative must:

- Be based in the same EEA country as the one in which some/all of the individuals whose data is being processed are based;
- Be appointed in writing to act on your organisation's behalf to deal with relevant data protection authorities (**DPAs**) and data subjects, although they can be an individual or entity (e.g. a law firm) and must have the capacity to represent your organisation; and
- Have their details included in relevant privacy notices and made accessible to supervisory authorities.

You do not need to appoint a representative if you are a public authority or if your processing of EEA Data is occasional, low risk and does not involve the large-scale use of special category or criminal offence data. For example, if a UK based football agent, who deals solely with British players playing in the UK, arranges a deal with an EEA based equipment supplier and they only process that supplier's business contact details, they would not need to appoint a representative. However, if the agent later begins representing a number of players from the EEA, the agent may well need to appoint an EEA representative.

3. *Supervisory Authority*

Since the introduction of GDPR, UK based organisations who undertake "cross-border processing" have had the benefit of the "one-stop-shop" system, meaning that the UK's Information Commissioner's Office (**ICO**) has been their sole DPA point of contact (or "lead supervisory authority") on matters relating to such cross-border processing. "Cross-border processing" in this context means where: (i) data processing activities are undertaken by an organisation's offices/branches in more than one member state; or (ii) the relevant processing is undertaken by a single office/branch in one member state but such processing substantially affects (or is likely to substantially affect) data subjects in more than one member state.

From 1 January 2021, where a UK based organisation has offices/branches in the EEA and which are continuing to undertake cross-border processing within the EEA, that organisation will need to identify which EEA based DPA will act as the lead supervisory authority for those EEA offices/branches, as the "one-stop-shop" system will continue to apply to their cross-border data activities. The ICO will no longer be able to fulfil the lead supervisory authority function in this context meaning the relevant organisation will need to deal with both the ICO and relevant EEA lead supervisory authority going forward. Where a UK based organisation (without EEA offices/branches) will be processing data in a way which will substantially (or is likely to substantially) affect data subjects in the EEA, it will need to deal with both the ICO and the DPAs in all EEA states where the relevant individuals are based.

RECOMMENDED STEPS/CONSIDERATIONS

- Look out for a UK adequacy decision, this will greatly reduce the amount of work required to remain compliant post-Brexit. In the background however, you should review current data flows from the EEA and ensure a lawful mechanism can be put in place with effect from 1 January 2021, if required. If you need to roll out a large number of standard contractual clauses (or other safeguards), our advice would be to prioritise transfers involving the largest volumes of personal data or those which involve the transfer of high risk data categories (i.e. special category or criminal convictions and offences data).
- Where you are newly relying on standard contractual clauses or binding corporate rules having not needed to previously, you should conduct a transfer impact assessment, to assess whether the data importer is able to comply with the obligations under the relevant transfer mechanism.
- At the next practicable stage, sense check and update agreements and policies – we expect any changes to agreements and policies will be minimal, largely changing definitions and updating international transfer provisions where relevant.
- Consider whether you need to appoint a European representative and consider any practical implications of your organisation's inability to rely upon the "one-stop-shop" system for cross-border processing.
- Update internal data protection procedures and policies as appropriate and consider training for staff, particularly for those whose roles involve the processing of EEA Data.
- Be aware that in the absence of an adequacy decision, overseas counterparties may try to negotiate the liability cap under contracts on the basis of UK third country status. They may also request that data is moved to servers within the EEA.

Please get in touch with our Data Protection team if you have any questions.

Sophie Wilkinson

Partner

sophie.wilkinson@onsidelaw.co.uk

Alex Brooks

Associate

alex.brooks@onsidelaw.co.uk