Data Protection update – May 2022

As a result of Brexit, the UK now has its own independent data protection regime. The EU GDPR no longer applies, and instead the UK is subject to the UK GDPR (and Data Protection Act 2018).

At the moment, the 2 regimes are the same, so if your business was compliant with EU GDPR, you may not need to make any significant changes to comply with the UK GDPR except in relation to international data transfers (detailed below). Over time, however, it is likely that the UK GDPR will diverge from the EU GDPR.

Below are some helpful hints for ensuring you're in the best position with regards to data protection compliance. You can also use the ICO website to find more information and guidance.

1. **Standard terms and conditions**

To prevent your business having to comply with 2 different regimes in the future, **your standard terms and conditions with clients and candidates / contractors should reference the UK GDPR** as the applicable data protection legislation, and not the EU GDPR. They should also be updated with the new data transfer process and documentation (see below). This is most important for future contracts, but for some key clients or suppliers you may also want to consider varying existing contracts (ie those already signed) to reference the UK GDPR.

2. **Policies and notices**

Ensure your data protection policies and documentation, including privacy notices to data subjects (whether candidates or your own employees etc) **reference the UK GDPR**. If you do, or are likely to, transfer personal data outside the UK, you may also need to update privacy notices in accordance with the new data transfer processes (see below).

3. **Data Transfers**

There are significant changes to the process for transferring personal data outside the UK. Your processes and contracts will need to comply with these additional requirements going forward. Data transfers to organisations outside the UK are restricted. A transfer is defined as "sending or making available personal data to another business or organisation" which is based outside the UK.

Transfers to employees of the same company but based in different countries is not restricted, but transfers between companies (or employees of those companies) in the same group is restricted because they are different legal entities. Transfers from one processor in the UK to another processor in the UK that is electronically routed via another country is also unrestricted.

All other types of data transfer are restricted and transfers can only be made in one of the following circumstances (and reasons for transfers must be considered in this order):

I. **The country you are transferring to has an "adequacy regulation" in place**. These are currently the same as all the countries with an EU adequacy decision, but note the countries with UK adequacy regulations are likely to change over time. The current list is

as follows: all EEA countries, Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay, Japan (transfers to private sector only) and Canada (only for data subject to Personal Information Protection and Electronic Documents Act (PIPEDA))

II. **The transfer is covered by appropriate safeguards**. The list of possible safeguards is below; however please note that just having these safeguards in place is not sufficient in itself, you must also **conduct a Transfer Impact Assessment (TIA)** to determine if the safeguards are really sufficient, taking account of the protections contained in that appropriate safeguard and the legal framework of the destination country (including laws governing public authority access to the data). The ICO does intend to release further guidance on this topic.

- **Standard contractual clauses.** This is the most likely option you will use and is explained in more detail below.
- Binding corporate rules which have been approved by the ICO (intended for multinational corporate groups). More information is available here
- Code of conduct that has been approved by the ICO (none have been approved as yet)
- Certification scheme approved by the ICO (none have been approved as yet)
- Legally binding instrument between public authorities (not likely to be applicable to your business)
- Administrative arrangements between public bodies (not likely to be applicable to your business)

III. **The transfer is covered by an exception**. Exceptions are to be used sparingly, not as a general rule for data transfers. They can only be used where there is no adequacy regulation and you cannot ensure adequate safeguards. There are 8 exceptions but I have included only the ones that may be applicable / appropriate to private companies.

- **Explicit consent from the data subject.** This is the most likely option you will use and is explained in more detail below.
- To make or defend a legal claim
- You have a contract with the data subject that actively requires you to transfer their personal data outside the UK. This option can only be used for occasional transfers and is not suitable to use for regular transfers. It must also be necessary for you to make the international transfer in order to enter into or comply with the contract.
- You have compelling legitimate interests. This option can only be used as a "one-off", is for truly exceptional circumstances, and must be notified to the ICO and the affected data subjects.

4. Standard contractual clauses (SCCs)

Many businesses currently use the EU standard contractual clauses as an adequate safeguard for international data transfers. However, the ICO have now developed new UK-centric SCCs. The templates are here.

Any contracts entered into before the end of December 2020 using the (then current) EU SCCs continue to be valid for data transfers under UK GDPR until 21st March 2024. However, the EU issued new SCCs on 4th June 2021 and these are not valid for data transfers under UK GDPR.

You must use the ICO SCCs for any contracts you enter into after 21st September 2022. You must also use the ICO SCCs for any contracts with clients that originally used the EU SCCs if those contracts continue past 21st March 2024.

Please be aware the **ICO SCCs cannot be incorporated via hyperlinks into contracts** in the way that the old EU SCCs could be (and the new EU SCCs also cannot be incorporated this way any longer). The Data Transfer Agreement must be filled out for each client or supplier to whom you transfer data internationally, and must be signed as a separate document in addition to your terms and conditions.

The ICO is currently drafting additional guidance for using the ICO SCCs – please check the ICO website regularly for updates.

5. Explicit consent for international data transfers.

If you choose to use explicit consent for the transfer of data internationally, you must follow the following conditions.

- The consent given must be specific and information, and you must provide the data subject with precise details of the transfer (you cannot have or use an overarching or general consent mechanism).
- You must tell the individual:
    - the identity of the receiver, or the categories of receiver;
    - the country or countries to which the data is to be transferred;
    - why you need to make a restricted transfer;
    - the type of data being transferred;
    - the individual's right to withdraw consent; and
    - the possible risks involved in making a transfer to a country which does not provide adequate protection for personal data and without any other appropriate safeguards in place.
- If the individual withdraws their consent at any point, you cannot transfer their personal data internationally from that date onwards. For this reason, using consent as a mechanism for data transfers is not recommended except in occasional circumstances.

6. Direct marketing

Marketing activities via electronic means (phone, fax, email or text) and cookie monitoring is still governed by PECR (Privacy and Electronic Communications Regulations) regardless of Brexit. The ICO has more information and guidance on PECR here.

7. Processing activities

You are still required by law to maintain records of all your processing activities. Now is a good time to review those records to ensure they are still adequate and relevant. As part of your processing activities, you are (still) required to conduct DPIAs (data protection impact assessments) on any new projects, systems, software or other methods of processing personal

data that are likely to result in high risk to individuals' interests. The ICO has a DPIA template that you can use here.

Checklist of actions:

1) We have updated all our data protection documentation to reference UK GDPR, not the EU GDPR.
2) Our standard terms and conditions with clients, suppliers and candidates reference the UK GDPR, not the EU GDPR.
3) We have updated our processes for international data transfers, including:
    a. Conducting TIAs for any transfers using "adequate safeguards"
    b. If using standard contractual clauses to justify a data transfer, we have implemented the new ICO SCCs (**mandatory for all contracts entered into from 21st September 2022 onwards**)
    c. We have noted all the client and supplier contracts which reference the EU SCCs and will amend them to incorporate the ICO SCCs before 21st March 2024.
4) We continue to document all our processing activities, including conducting data protection impact assessments (DPIAs) where required
5) We continue to comply with PECR for direct marketing activities and website cookies.

If you need any additional information, or require help and support with any of the above, please contact bernie@labvolution.com.