Employee Data Privacy – United Kingdom

Cross-Border Data Transfer

Are there any restrictions on transferring personal data and how can these be overcome?

Cross-border data transfers affect all organizations that engage online IT services, cloud-based services, remote access services and global HR databases. Understanding the applications of lawful data transfer mechanisms is essential to validate recipients located outside the United Kingdom. Data transfers typically include the following examples:

- Personal data communicated over the telephone, by email, fax, letter, through a web tool or in person to a country outside the UK;
- IT systems or data feeds which lead to personal data being stored on databases hosted outside the UK;
- people/entities outside the UK being able to access or "see" personal data held in the UK; and
- the use of personal data by third parties through external solutions, e.g., outsourcing, offshoring and cloud computing.

Cross-Border Data Transfers

Requirements to transfer personal data outside the UK is governed by the UK Data Protection Act 2018 (UK GDPR), and largely mirrors the European Union's General Data Protection Regulation requirements. It is important to note that the transfer of personal data to a third country or an international organization is possible. The transfer is legally allowed where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection. A transfer based on a decision of adequacy shall not require any specific authorization.

Data transfers between the UK and EU member states is currently unrestricted. In June 2021, the European Commission granted an adequacy decistion to the United Kingdom.

In the absence of a decision of adequacy, the personal data transfer to a third country may take place if appropriate safeguards are in place, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Examples of measures that can be taken include:

Binding Corporate Rules (BCR): personal data protection policies offer clear sets of rules for businesses engaged in a joint economic activity. They are adhered to by a controller or processor established in the country for transfers of personal data to a controller or processor in one or more third countries.

The BCR must contain: privacy principles (transparency, data quality, security, etc.); tools of effectiveness (audit, training, complaint handling system, etc.); and an element proving that BCR are binding. BCR must be submitted to the UK ICO for approval.

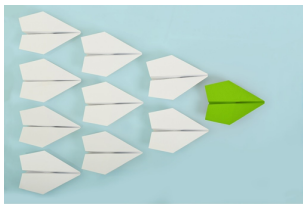
Standard Data Protection Clauses: clauses that offer sufficient safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals. Standard data protection clauses impose contractual obligations on the sender and the receiver, and grant rights to individuals whose personal data is transferred. Individuals must be able to directly enforce those rights against the sender or receiver, or both. The ICO has issued two sets of standard data protection clauses: (i) an International Data Transfer Agreement (IDTA) and (ii) an International Data Transfer Addendum (Addendum).

The Addendum is an addition to the EU GDPR standard contractual clauses (SCC) that enables organisations to rely on the EU's new SCCs, which were issued in June 2021.

If organisations entered into the old EU SCCs prior to 21 September 2022, these old EU SCCs will continue to be valid for international transfers under the UK regime, but only until 21 March 2024. From 21 March 2024, if the international transfers continue, orgnaisations must enter into a new contract on the basis of the IDTA or the Addendum.

Standard data protection clauses are not subjected to any authorities' approval, the main reason why their content cannot be modified. If changes are made, the parties must submit the document for ICO approval.

Adopting BCR, IDTA and the Addendum allows organizations to harmonize practices relating to the protection of personal data within a group, avoid the need for a contract for each single transfer, communicate externally on the company's data protection policy, have an internal guide for employees with regard to personal data management, and make data protection integral to the way the company carries out its business.



HR Best Practices:

For intragroup transfers (such as access from a subsidiary outside the UK), make sure to have at least one safeguard mechanism in place: BCR "Controller to Controller" or Standard data protection clauses signed with the concerned subsidiary. For cross-border data transfer with processors or sub-processors, make sure such collaborators have their own safeguard mechanisms in place.

The use of applications in the cloud frequently results in the international transfer of employee data. Personal data should only be transferred outside the UK when an adequate level of protection is ensured and access by subsequent entities remains limited to the minimum necessary for the intended purpose.

Last updated May 2023.