

Data Protection in 2010

Workshop F - Introduction to international data transfers

Outcomes

Aims

The aim of the workshop was to give an introduction to international transfers, covering hot topics such as binding corporate rules (BCRs – binding codes of corporate conduct allowing companies to transfer data internationally within their group) and model contracts, plus a look to the future.

The ICO's role in relation to international transfers includes the provision of guidance to organisations at various levels, which are detailed in the workshop slides. The Information Commissioner also has the power to approve international transfers of data, but does not generally do so unless in exceptional circumstances. This is because he considers data controllers themselves to be in a better position to decide on the adequacy of protection with regard to individual international transfers.

However, the ICO does have a specific role in granting authorisations of BCRs.

International transfers and the law

Article 25 (1) of Directive 95/46/EC states that "Transfers must only take place to a third country providing an adequate level of protection".

The 8th Data Protection Principle of the DPA98 states that "Personal data shall not be transferred to a country or territory outside the EEA, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data".

The emphasis on 'adequacy' can be noted.

Recommended approach

The ICO has produced a 10-point checklist which sets out a recommended approach to compliance with the 8th principle.

1. Do you need to transfer personal data? Can the data be anonymised for example? Is a transfer a proportionate response to the issue?
2. Is there a transfer? Consider transit – for example, if data is transferred electronically from country A to country B, via a server in country C, there is no transfer to country C, only transit. For there to be a transfer data must have been sent to that country in order for something to happen to it there. Another example would be a business trip to New York where the businessperson takes their laptop, but does not plug it in or transmit any data from there – no transfer has taken place. There is, however, case law with regard to the internet. If personal data is loaded onto a UK server and subsequently accessed by someone abroad, technically a transfer has taken place. A final consideration is where information not classed as personal data (for example, certain types of manual data) is transferred outside the EEA with the intention of inputting it on a computer system – if the intention is that the data will be held as personal data after the transfer, then a transfer of personal data is deemed to have taken place.
3. Have you complied with the other data protection principles? All the data protection principles have equal weighting and must all be considered. In the New York business trip example, even though no transfer actually takes place the other principles must be complied with – for example customers should have been informed beforehand of the possibility that their personal data may be transferred outside the EEA.
4. Is the transfer to a country outside the EEA? The EEA includes all EU member states plus Iceland, Norway and Liechtenstein, and data can be transferred between EEA member states without engaging the 8th principle.
5. Has there been a finding of adequacy by the EU Commission of the destination country? If the destination is outside the EEA, there may be a finding of adequacy under Article 25 of the Directive. Countries currently considered to have adequate levels of protection are Argentina, Canada, Jersey, Guernsey, Isle of Man, Switzerland, Israel and Andorra.

6. Is the transfer to a member of the US Safe Harbor scheme? If the transfer is to the USA (which has no finding of adequacy) then the recipient organisation may be a member of the Safe Harbor scheme. The scheme is a voluntary one with seven principles very similar to the eight principles in the DPA98. It is, however, limited to certain sectors – for example, telecoms and financial services sectors cannot join. If an organisation is a member, transfers can be treated as if there was a finding of adequacy.
7. Can you assess adequacy in line with schedule 1, part 2, paragraph 13 of the DPA98? This includes considering both legal adequacy (such as the law in force in the recipient country, international obligations, whether the rule of law exists) and general adequacy (such as the nature of the data, its intended use and the risks inherent in this – for example an internal telephone list as opposed to confidential health records). The country of origin is also relevant as expectations of data subjects in different countries may vary. Whether the business is setting up a permanent system of data transfers or whether the transfer is a one-off is also relevant.
8. Can you put in place adequate safeguards by the use of model contracts / BCR (for intra-group transfers)? If the previous step shows gaps in adequacy, model contractual clauses as approved by the EC and the ICO may be used. There are contracts covering data controller to data controller transfers and data controller to data processor transfers. The contracts place obligations on the 'exporter' and the 'recipient' and give enforceable rights to data subjects. It should be noted that model clauses cannot be changed. However, if the model clause wording remains unaltered but further clauses are added, the contract will no longer be an approved one but will be adequate. There are new contract clauses for controller to processor transfers in operation from 15 May 2010.

BCRs can be used for international transfers within a multinational group. Organisations apply to the relevant European data protection authorities for approval – the lead authority being the country in which the organisation conducts most of their business.

Some delegates commented about the length of time BCR applications take, and suggested that this puts off many organisations from applying. The ICO together with other

European DPAs are trying to streamline the process – previously applications were assessed under the co-operation procedure whereby once the lead DPA was satisfied of the adequacy of the application it was circulated to other European DPAs for comment. This sometimes took a considerable length of time. A newer system of ‘mutual recognition’ is increasingly being used for BCR application assessments, which allows for BCRs to be authorised without comments from all involved DPAs – with reviews from just two other DPAs after the lead authority is satisfied the code is adequate.

The definition of ‘multinational’ was questioned and it was stated that for organisations such as charities which may have several offices across the world but are not single companies, some sort of inter-group agreement could be used. As long as all parts of the organisation can be bound by the code then BCR could be a possible route.

9. Do any of the schedule 4 derogations apply? The first of these is consent, although it was stressed that individuals must have given consent as defined in the Directive (freely given, specific and informed). It is the responsibility of the data controller to prove that the data subject understands what they are agreeing to, and that the consent has been freely given – so in situations where a business transaction cannot be carried out without consent, the derogation does not apply. The Article 29 working party view is that there are inherent difficulties with consent in this context.
10. Have you recorded the basis on which you made your decisions? This was stressed as very important.