

Data Protection Officer Conference

Afternoon workshop E1
Principle 8: An overview



Questions and answers

Q1. Where can I find the list of adequacy findings?

A1. They are on the ICO and the Commission's websites.

Q2. Some companies certify themselves as part of the Safe Harbor scheme for their own data but they are not certified for 3rd Parties data. Isn't this misrepresentation?

A2. It could be if it is misleading. You can report this to the Federal Trade Bureau.

Q3. Would you recommend using model contract clauses with a Safe Harbor company if the transfer is from somewhere that does not regard Safe Harbor as enough?

A3. That is one option.

Q4. What is the ICO view of The Patriot Act?

A4. This Act allows some US authorities to access data. However, most countries have the possibility for access by the security services or secret services. If there is a serious risk that the Act would be applied to the entity receiving the data then it will be a factor to be taken into consideration when assessing adequacy.

Q5. If there was an incident involving a processor outside the EEA would the Commissioner look for evidence of an adequacy assessment?

A5. Yes (unless model clauses had been used), and we would look for a Principle 7 processor contract.

Q6. What happens if a processor has accepted model clauses but with a low limited liability?

A6. This does not limit the liability as between the data controller and data subject, it merely limits the amount the data controller can claim from the processor.

Q7. What is meant by “necessary” in the context of the derogation relating to performance of a contract?

A7. It does not mean necessary just because of how you choose to structure your business i.e. you choose to outsource there. It means necessary in that the contract cannot be fulfilled without it. E.g. if ordering goods from overseas you have to give your name and address for delivery, or in making an overseas hotel booking you have to give the hotel the name of the occupant.

Q8. Is it a view specific to the ICO that transfers to processors as opposed to other controllers are likely to be less problematic?

A8. Yes. Our view is that as the data controller retains control issues regarding the processing are more likely to be about security rather than ability to transfer.

Q9. If you are able to see the data in another country does that amount to processing and a transfer?

A9. Yes, it is likely to be a transfer, particularly if you are able to manipulate the data from overseas.

Q10. If you have a system that everyone can view data, even if the server is in the UK, is it a transfer?

A10. If you can do something with the data then yes but as it is within the same organisation and you will all be bound by the same rules it should be quite easy to make a finding of adequacy.

Q11. If it is view only is it still a transfer?

A11. In our view, yes. It is best to act with caution.

Q12. Does the ICO need to sign off on an adequacy finding?

A12. No. Other countries do but we only review and authorise BCRs.

Q13. If you have a data controller/data processor relationship with a 7th principle contract in place what steps are needed to comply with principle 8?

A13. It is up to you. You can use model clauses, a BCR or an adequacy assessment (assuming the processor is outside the EEA).

Q14. Executives travel overseas with i-phones and i-pads from which they can access emails using wi-fi. Is there a principle 8 issue?

A14. This is more to do with security. If you put safeguards in place then you can assess it as adequate anyway. We would agree that if you they are travelling to countries that are encryption averse then they probably shouldn't be taking them.

Q15. When you are looking at transfers to big organisations like Google how can you assess adequacy when they won't alter their standard contractual clauses? What rights of audit are there?

A15. If the organisation is in the Safe Harbor scheme then you have adequacy for the transfer but otherwise you have to find a way to ensure adequacy depending upon what you are transferring and why. Document your findings.

(A comment was made from the delegates that some organisations do have independent audits carried out that are published (CAS 70) and you can rely on this to some extent but we acknowledge this lack of audit power is a potential problem and will increasingly become so with cloud computing.)

Q16. Could the Foreign Account Tax Compliance Act in the US be a data protection problem?

A16. This enables the US tax authorities to obtain access to personal data about a US national that is held outside the US in order to tax them. A body that does not comply with a request for data can be fined by the US and a body that does comply may be in breach of European data protection legislation.

There is an Article 29 subgroup looking at this issue and attempting to find a way forward but it is acknowledged that there is a potential problem to be looked at here but all countries are working together to try to find a way through.