Feedback on the EDPB Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data by the Law Society of England and Wales and the Law Society of Scotland

December 2020

INTRODUCTION

1. This paper sets out the views of the Law Society of England and Wales and the Law Society of Scotland on the draft recommendations of the European Data Protection Board (EDPB) on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
2. The Law Society of England and Wales is the professional body for the solicitor profession in England and Wales, representing over 160,000 registered legal practitioners. The society represents the profession to Parliament, government and regulatory bodies and has a public interest in the reform of the law. This response has been prepared by the Law Society's Technology and Law Committee.
3. The Law Society of Scotland is the professional body for over 12,000 Scottish solicitors. It sets and upholds standards to ensure the provision of excellent legal services and ensure the public can have confidence in Scotland's solicitor profession. It has a statutory duty to work in the public interest, a duty which it is strongly committed to achieving through its work to promote a strong, varied and effective solicitor profession working in the interests of the public and protecting and promoting the rule of law. It seeks to influence the creation of a fairer and more just society through active engagement with the Scottish and United Kingdom governments, Parliaments, wider stakeholders and its membership.

EXECUTIVE SUMMARY

1. We welcome the EDPB's recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. In particular, we welcome the clarifications on:
   - additional safeguards to be used by exporters; and
   - application of these safeguards to all transfer tools under article 46 of the GDPR.
2. We would, however, like to point out two key areas that would benefit from further discussion:
   - the current requirements to assess the laws and practices of a third country which are likely to be extremely difficult for most organisations;

- there are several inconsistencies between the current drafting of the proposed standard contractual clauses (New SCCs) and the drafting of the EDPB recommendations.

3. Therefore, we recommend that the EDPB develop:
   - a knowledge bank of country-specific information and guidance;
   - more specific guidance on compliance measures for SMEs, recognising the compliance challenges facing SMEs; and
   - further guidance on notification to supervisory authorities where there may be more than one authority.
4. In addition, further guidance or examples of onward transfers may be helpful.
5. We also recommend the EDPB and the Commission work together to clarify inconsistencies between the current drafting of the recommendations and the New SCCs.
6. Finally, we would like to suggest the EDPB considers wording that would require data exporters to use 'appropriate' technical standards, such as encryption, in line with Article 32 of the GDPR, as opposed to the currently recommended best possible standard.

GENERAL REMARKS

1. If we look at the current business environment, we can see the increasing importance of guidance on the cloud services, remote use and data transfers for support purposes which many international firms use on a daily basis.
2. We **welcome** the recommendations' emphasis on the minimisation of data being transferred and reviewing any access/permission requirements.

COMMENTS ON STEP 3

3. We would like to point out that the requirements set out in Step 3 (transfer impact assessment) of the guidance are likely to be extremely difficult for most organisations.
4. First of all, the assessment of laws and practices of third countries will require a substantial degree of investigation which may be cost and time prohibitive for private entities, particularly SMEs. In addition, we believe that listing of what is seen to be relevant national legislation is not the same as how authorities decide to invoke or interpret particular provisions of relevant legislation and the kind of data processing it applies to.
5. We would therefore **welcome** further guidance on how SME data exporters can comply with the new requirements.
6. Secondly, such assessments are likely to vary between organisations due to the range of sources regarding law and practice (and entities' access to such sources), and their interpretation of the political situation. Such divergence does not deliver much anticipated legal certainty for businesses.
7. We **recommend** the EDPB builds up a knowledge bank of country-specific information and guidance over time. It should also consider other measures that

would help organisations in assessing the laws and practices of third countries (e.g. a checklist or template for such an assessment).

8. To further illustrate the points made above, one can again look at the current drafting of the proposed New SCCs (to which the EDPB recommendations apply) which requires the parties to work together to document the assessment (section II, clause 2(d)). This is likely to be difficult in practice for example due to the potential conflict of interest or differing views. It is possible that the importer and exporter each produce their own assessment based on their interpretation of the evidence. It is equally possible that the importer provides a 'one to many' assessment package and the exporter disagrees with the analysis.
9. Thirdly, in the current draft of the recommendations and New SCCs it is not clear whether subjective factors are allowed to be taken into account in the assessment of local laws.
10. By way of illustration, Section II, clause 2 (b)(i)) appears to allow for the consideration of subjective factors by evaluating '*relevant practical experience indicating the existence or absence of prior instances of requests for disclosure from public authorities received by the data importer for the type of data transferred*.'
11. However, the EDPB warns data importers away from '*subjective factors*,' including '*the likelihood of public authorities' access to your data in a manner not in line with EU standards.*'
12. We **recommend** that there be consistency between the requirements of the New SCCs and the EDPB the guidance on which factors should be taken into account.

COMMENTS ON STEP 4

13. We **recommend** developing further guidance on the appropriate competent supervisory authority to notify of an importer's inability to comply with a contract. Where there are multiple authorities, each with the power to impose fines, it is currently unclear which should be notified.
14. We would like to **note** that there may be significant practical difficulties in extrapolating data where the circumstances require the data transfer to cease/be suspended and the data to be destroyed or returned to the data exporter (para 52). This is not always possible or straightforward.

COMMENTS ON TECHNICAL MEASURES

15. We think that the recommendations set very high standards in the use cases around encryption. It is worth bearing in mind that organisations will often transfer data to non-EEA countries where the risk of access to data has been identified as low. We would therefore **suggest** that the recommendations require 'appropriate' technical standards, such as encryption, in line with Article 32 of the GDPR.
16. We **welcome** the acknowledgment of the effectiveness of 'additional contractual measures' (from para 92 onwards) but would **point out** that they may be limited by the national law or regulation. In our view, this shows the difficulty of creating lengthy and potentially unenforceable clauses.

17. It is possible that a data importer may have personal security concerns in signing up to these clauses. For example, was the "canary warrant" envisaged as an outcome of the Schrems II decision? When would the local data importer be in a position to reveal the existence of a backdoor or business process being manipulated by public authorities? We would **welcome further clarity** on this issue.
18. The scenarios 6 and 7 given by the EDPB may apply to cloud providers and many global companies that share resources (IT infrastructure) or management functions (HR or marketing) across borders.