Centre for Information Policy Leadership
Hunton & Williams LLP

The "One Stop Shop" – Working in Practice

Introduction

This paper is submitted to the Working Party in light of its deliberations on the application of the One Stop Shop ("OSS") under the proposed General Data Protection Regulation. It is based on work carried out by Rosemary Jay, Senior Attorney at Hunton & Williams, and on her full article, published on the 3 November by the Society for Computers and Law at http://www.scl.org/site.aspx?i=ed39323. We would be happy to explore, explain or debate the proposal further under the aegis of the Centre for Information Policy Leadership at Hunton & Williams. The paper aims to offer a vision of the OSS which balances the concerns and the aspirations of all those involved in the process to provide a practical, flexible and effective solution.

Summary

The Council has carried out significant work on the role of the supervisory authorities, but the OSS remains an issue of substantial debate.

This paper suggests some fresh thinking on the OSS which is intended to:

- ensure that the OSS concept is workable and effective in practice;
- allow the OSS to develop and strengthen further over time, as the experience in implementing the concept grows; and
- incentivise controllers to commit actively to pan-European compliance.

The proposal is a good "fit" with the existing work on the arrangements for cooperation between supervisory authorities and the development of the consistency mechanism. It could be integrated into the current draft with minimal effort.

In brief, the suggested approach recognises – and builds on – the benefits of the OSS to controllers from the certainties and cost-savings of dealing mainly with a single supervisory authority. But, instead of a model imposed automatically on controllers with cross-border activities, it suggests the OSS as an agreement between controllers and supervisory authorities incorporating legally-binding, tailored commitments by data controllers. Under these agreements a data controller will undertake to accept specified actions to ensure:

- observance of any order from the lead authority by all its relevant establishments throughout the EU; and
- that individuals affected by its processing will be properly protected and can freely exercise their rights in their local jurisdictions.

Drawing on the BCR model for international transfers, such an OSS model would be a formal arrangement backed up by a legal structure.

Changing the perspective

There is a need to place more explicit focus in the complex OSS discussions on an active role for data controllers. This must complement debate about the role and powers of regulators and the position and rights of data subjects. In practice, it will be data controllers who will have the primary responsibility for making the law work, delivering individual rights, building compliant businesses and communicating with data subjects. The OSS would thus be re-designed to incentivise data controllers to be committed, engaged and have an active role in building and delivering compliant solutions.

Problems with current proposals

Current texts present various problems which risk the effective operation of the OSS. These include:

- The application of the OSS is automatic**,** with a "one size fits all" approach which ignores numerous different business models;
- The automatic application of the OSS will impose significant burdens on supervisory authorities, which they may struggle to manage and resource;
- If a data controller has multiple establishments in the EU, the OSS is imposed irrespective of the legal or practical ability of the main establishment to control other establishments;
- Data controllers have no obligation or incentive to take an active role in the operation of the OSS or in ensuring pan-European compliance. The obligations of a data controller subject to an OSS are exactly the same as any other data controller, e.g., there will be no formal obligation to provide additional or more detailed information to the lead supervisory authority;
- The OSS appears to be inflexible. There is no provision to alter the nature or terms of the OSS, due to specific processing activities by controllers, changes in the context and wider environment; and
- The system has a degree of rigidity that may make it difficult to take advantage of future learning, development and modification of the concept.

Suggestion

A well-designed OSS should bring real benefits to data controllers, to supervisory authorities and to data subjects. It should make the attractions to data controllers (notably certainty and cost-saving) available as an inducement in exchange for active engagement in ensuring that data protection is delivered as a reality regardless of jurisdiction.

It is suggested therefore that the Regulation should provide for the OSS to be an option to data controllers and regulators. It should be available with the positive agreement of the relevant supervisory authorities, but only to those controllers who are prepared to take additional steps to engage with regulators in making it work. A data controller should not be entitled to take the benefit of an OSS without offering appropriate assurances that it is committed to working in partnership with the relevant supervisory authorities.

An outline of the suggested process is set out below. While the concept would require some additional development, the core idea is for the OSS to operate as a formal arrangement between a controller and a supervisory authority, backed up with a legal structure and based on the following:

- The process to initiate the OSS could be put in motion by either the supervisory authority, inviting a data controller to apply for the OSS, or the data controller, applying for the OSS.

- The data controller would make an application through its "lead establishment" to one "lead authority". The "lead establishment" would be based on criteria similar to those currently used for determining the lead authority for the BCR application process. The application would specify the data processing for which the controller wishes to establish the OSS (the scope of OSS), the location of its other establishments in the EU and the actual criteria used to determine the appropriate lead authority.

- The application, tailored to the circumstances of a specific controller, would also include the following assurances:

    - demonstrating how the controller will be able to take effective measures to allow the individuals the exercise of their rights in other jurisdictions, e.g., that local offices will deal with the exercise of rights or complaints in the local language, cooperate with the local supervisory authority over local investigations, and deliver local solutions;

    - stipulating how the controller will establish reporting and liaison arrangements with the lead authority, including a regular report of all local matters dealt with local supervisory authorities (e.g., complaints received in the EU);

    - putting in place corporate arrangements to exercise real control of all the relevant processing (in scope of OSS) carried out in its other EU establishments, with the ability to deliver compliance in respect of all such processing; and

    - guaranteeing to deliver compliance in all its EU establishments with any order served by the lead authority.

- On receipt of the application, the prospective lead authority would consult with the relevant local supervisory authorities and could reject the application for good cause and/or pass it on to another supervisory authority.

- Upon agreement of the arrangements, the scope of OSS and the assurances would be set out in a formal and binding undertaking from the controller which would remain in force for a set period of time. In return, the OSS arrangement will be recognised by all the affected supervisory authorities.

- The lead authority would have the main competence for supervision over the processing in scope of the OSS, but local supervisory authorities would be competent to deal with individual complaints locally.

- The lead authority would operate as a central point of knowledge and liaison with the controller. It would deal with those matters which have a cross-border aspect, including the grant of prior authorisation, prior consultation for new processing, guidance and advice to the business, receipt of security breach notifications and determining whether notice should be provided to data subjects. It would also be empowered to enforce measures having a cross border aspect.

- The lead supervisory authority would be able to seek the cooperation of the other relevant supervisory authorities, e.g., in conducting local investigations or carrying out routine audits. The lead authority would be responsible for reporting on its supervisory activities in respect of the controller and making information available to the other relevant supervisory authorities.

- If the lead supervisory authority issued an order or an enforcement action against the controller requiring actions by any of the other establishments, a failure by the local establishment to comply would result in sanctions against the lead establishment (including the withdrawal of the recognition of the OSS).

- At the end of (say) a three-year period, the OSS arrangement would be reviewed by the controller and lead authority, and could be renewed or re-negotiated.

The BCR precedent

BCR have been developed to provide practical and deliverable compliance in co-operation with data controllers. An OSS recognition would not require the same level of detail as a BCR application, but would utilize the same concept of using a binding legal commitment from the data controller to work with the regulators within a statutory scheme.

Consultation and co-operation between supervisory authorities

Any OSS arrangement must provide for proper consultation and co-operation between supervisory authorities, as the other authorities would be expected to advise and support the lead authority in its role. To ensure effective operation of OSS and less strain on resources, in appropriate cases, this support could be formalised through a smaller Advisory Group of supervisory authorities (2-3 other authorities in addition to lead authority). In the event of a real dispute between supervisory authorities the consistency mechanism would be available. Another option is that EDPB could act as a mediator.

Costs

The adoption of any OSS would put a strain on the lead authority. It would be reasonable to require the data controller to pay a fee to the lead authority, for the operation of OSS.

One of the benefits of this suggestion would be that OSS arrangements would be developed gradually, as more and more data controllers see the benefits. In this way, supervisory authorities would not be faced with the immediate burden of operating the OSS for all eligible data controllers on entry into force of the Regulation.

Conclusion

The concept of a lead authority to deliver robust and effective regulation across Europe, while at the same time offering certainty and clarity for business, is powerful. It also serves the needs of data subjects, while enabling the growth and competitiveness of digital Europe. In practice, this concept will work best with the active and demonstrable engagement of businesses who submit to a lead authority and are able to commit to delivering compliance across the EU.

Rosemary Jay – Senior Attorney, Hunton & Williams, and the author of Sweet & Maxwell's book Data Protection Law & Practice, and an editor of the Encyclopedia of Data Protection and Privacy
Bojana Bellamy – President, Centre for Information Policy Leadership at Hunton & Williams
Richard Thomas – Global Strategy Advisor, Centre for Information Policy Leadership at Hunton & Williams

The views expressed in this paper are those of the author and collaborators only and should not be taken as the views of Hunton & Williams LLP, the Centre for Information Policy Leadership or its members. We are grateful for those who have provided insights and feedback in the process of developing this paper. We recognise that the proposal is, at this stage, an outline one and will be conducting further work to refine and improve the concept subject to continuing feedback.