TRUATA.

A post-Schrems II world:
5 insights for international data transfers

The European Data Protection Board (EDPB) has released Recommendations on additional measures that businesses now need to put in place to conduct lawful international data transfers.

Since the landmark CJEU 'Schrems II' ruling in mid-July, businesses have been grappling with the unknown and trying to navigate the uncertainty around how lawful international data transfers will be conducted moving forward.

This long-awaited guidance from the European Data Protection Board (EDPB) has now been delivered through a 38-page outline of Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of data protection. And, the clear takeaway message is this: organizations must now adapt and transition to the new world we are living in; a world that places privacy at the forefront of commercial conversations, transactions and transfers.

Where Safe Harbor and the Privacy Shield have previously failed, the Standard Contractual Clauses (SCCs) are here to stay— although with some caveats. And, from an organizational perspective, they will be one of the most viable and frequently used mechanisms when transferring personal data internationally. However, these SCCs will now, in most cases, require supplemental safeguards to be put in place by organizations in order to ensure that the level of protection of personal data is essentially equivalent to that guaranteed in the EU by the GDPR.

What does this mean for organizations needing to transfer data internationally?

While some may have hoped that the eagerly anticipated guidance would enable data to continue to flow with relative ease, the EDPB have laid out, what is effectively, the new playbook for our Post-Schrems II world – a playbook that requires operational change to ensure a consistent level of protection for data being transferred outside of Europe and a new way of ensuring that data protection is baked in at the organizational core.

The time has come to move away from a 'wait and watch' approach that hinges on hope for workaround solutions; it is imperative that businesses now act with agility in order to transform, adapt and ensure they are operationally ready to tackle international data transfers in a way that they haven't had to do so before.

1. ‘Business as usual’ is no longer the status quo

From an organizational perspective, there is likely to be a seismic shift in the way many businesses operate to ensure that transfer processes are efficient, compliant, and commercially valuable.

The EDPB’s Recommendations confirm a hard stop for non-compliance and drills home a message of accountability that every organization must attune to. The Recommendations make it clear that a ‘cease and desist’ approach to data transfers will apply in cases where an essentially equivalent level of protection cannot be guaranteed.

Therefore, when it comes to adhering to the EU levels of protection of personal data, there really is no compromise; companies must embrace the new privacy-focused world. And, in the case where current transfers do not achieve the required level of protection, organizations must implement new supplementary solutions or cease activity.

These solutions may involve anonymizing or pseudonymizing data or aggregating data prior to transfer, synthesising data, or retaining data in the EEA while providing privacy-preserving access to external analysts.

The commercial reality here is that this is no simple task; the supplementary measures that companies need to implement, above and beyond SCCs, will be a huge drain on time and resources. There will be a lot more overhead on the data controller to make sure that they have the right measures in place.

However, it will be the organizations that understand that this is a transition to a new way of working for the long term, and those that look to prioritize putting new measures in place, who will find themselves much better placed than the organizations playing catchup later on.

2. Organizations need to assess vulnerabilities and take action

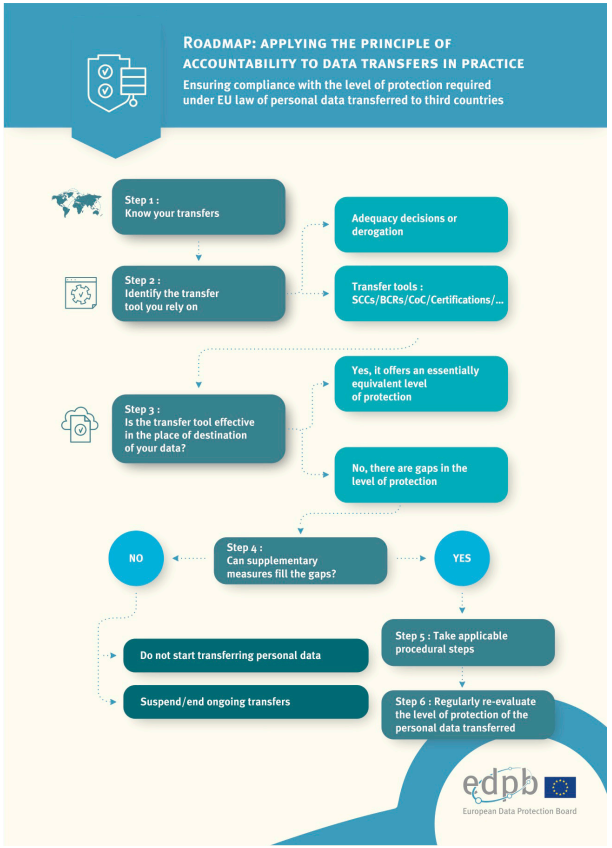
Rather than being a point-in-time process, the EDPB's Recommendations require organizations to bake data protection into all steps of the data transfer journey – from today. As such, organizations must now set out privacy-enhancing initiatives for all transfers and all processing activities. This requires immediate data mapping to establish where the vulnerabilities are in the data flows. It is an operational overhaul that calls for transparency, effective reporting and continuous assessment.

And while this should come as no surprise, since this is the direction that data protection law has been moving in for the past few years, it does require a top-down approach. In much the same way that data quality programs are implemented and operate on all data being handled in an organization, privacy processes must be applied to data at rest, data in transit and data in use. Given that data flows and data processing requirements change over time, organizations will also need to lay out a risk-based approach for reviewing and updating their processes regularly.

To assist organizations with an actionable 'what now?' way forward, the Recommendations outline a six-step roadmap that must be followed to determine what further actions need to be taken prior to transferring personal data outside the EEA.

What is clear from the Recommendations is that the EDPB understands the need to provide guidance to organizations on how to conduct their international transfers; as such, it has been helpful in providing a menu of options that businesses can put into practice, all while placing data protection at the heart of how they operate.

However, in providing such a roadmap, there is also a clear reinforcement of the levels of accountability and responsibility being placed on organizations; not only will they need to ensure the level of required protection is met when data is being transferred to a third country, but they will also need to have the evidence of the steps taken when evaluating the lawfulness of the transfer process.



3. When it comes to additional safeguards, one size does not fit all

International data transfers bring with them a number of complexities that require organizations to consider what the country-specific impact is for each transfer.

And when it comes to data transfers, each purpose will require organizations to adopt solutions that are fit for that specific purpose. Put simply, there is no one-size-fits-all approach to transfers that can tick a generic compliancy box.

Organizations will now need to carefully consider a number of different factors and transfer tools – such as SCCs, Data Protection by Design and Data Protection by Default, supplementary safeguards and localized processing – to establish what approach enables them to balance data protection with data processing.

Even where pseudonymization is used as a technical supplementary measure, "simple" or "basic" pseudonymization will rarely be sufficient. Organizations will need to look at enhanced pseudonymization techniques that can transform the data in such a way that it can no longer be attributed to an individual without the use of additional information, and provided that additional information is held exclusively by the data exporter.

So, while the EDPB's Recommendations does provide guidance and examples of personal data transfers which, together with a non-exhaustive list of supplementary measures, could provide essentially equivalent protection, organizations will need to conduct a **Transfer Impact Assessment** (TIA) for each unique transfer. In some cases, they may conclude that the international transfer can go ahead and in other cases they may conclude that the transfer may only go ahead if they put in place supplementary technical measures – and in some case with additional contractual or organizational measures - to achieve essential equivalence.

Ultimately, organizations will need to seek out the right legal and technical expertise and solutions that can assist them with more complex transfer operations.

4. Adopting a proactive approach to PETs will open up commercial opportunities

There's no escaping the fact that conducting a thorough Transfer Impact Assessment (TIA) for each unique transfer route, and monitoring it regularly, will not only create a lot of initial work, but a lot of ongoing work for organizations.

When it comes to protecting personal data, the job is never quite 'done', and in many cases, the complex nature of international data transfers will require expertise that go far beyond what may typically exist in most businesses, even those that are fortunate enough to have an experienced data protection team.

This is why so many organizations are quickly turning to privacy-enhancing technologies (PETs) that can automate and identify hidden re-identification risks, mitigate such risks and provide audit trails of evaluation processes – or even go a step further in offering a pseudonymized data solution for international transfers.

Organizations are also realizing that an early adoption of PETs in overcoming the challenges presented by international transfers can, in fact, open new revenue opportunities.

Yes, a forward-thinking data strategy not only leads to a solid position from a compliance perspective, it also presents organizations with opportunities to innovate and drive commercial growth.

5. There is no transition period and strategic confidence is key

Lastly, it is imperative for organizations to understand that there is no transition period from the CJEU's decision on Privacy Shield or SCCs, nor is there any grace period for the EDPB's recommendations.

While there is a consultation period for EDBP recommendations until November 30th, this is likely more of a refinement process rather than an opportunity for overhaul. Typically, consultation periods do not deliver any huge changes, but rather clarify on phrasing and definitions. So, while there may be a temptation for organizations to 'sit back and wait a little longer', this may not be the best transition strategy.

In the same way that data quality programs apply to all personal data handling and processing activities, a consistent set of strategies for Data Protection by Design and Data Protection by Default give an organization the confidence that it is operating in compliance with the law. Therefore, it is the organizations that adopt such strategies that are future-proofing their business.

Organizations now need to put in the effort to back what the GDPR intended: the protection of European citizens personal data to European standards—irrespective of the location of the data.

If anything is undeniably clear from the CJEU'S Schrems II ruling and from the EDPB's Recommendations, it's that there must now be a 'before' and 'after' when it comes to ensuring an essentially equivalent level of protection for the use and movement of personal data that are subject to international transfers.

With technology trends in privacy-enhancing computation and hyperautomation continuing to evolve the data landscape, it will be those organizations who invest in forward-thinking data strategies and leverage tech solutions to solve complex data handling that will reap the rewards by pushing back the walls which, during the clouded uncertainty following the Schrems II ruling, seemed to be closing in on them.

Timing is everything and action is required now if organizations want to continue operating on a global level.

Get started today by tapping into our expertise and solutions. We're here to help.

Find out more at truata.com