phg foundation
making science work for health

Impact of Schrems II

on sharing genomic data

UNIVERSITY OF CAMBRIDGE

Authors

Johan Ordish and Alison Hall

This report can be downloaded from:
www.phgfoundation.org

Published by PHG Foundation
2 Worts Causeway
Cambridge
CB1 8RN
UK
+44 (0)1223 761900

August 2020

Correspondence to:
intelligence@phgfoundation.org

PHG Foundation is an exempt charity under the Charities Act 2011 and is regulated by HEFCE as a connected institution of the University of Cambridge. We are also a registered company No. 5823194, working to achieve better health through the responsible and evidence based application of biomedical science

Impact of *Schrems II* on genomic data sharing

On 16 July 2020, the Court of Justice of the European Union (CJEU) handed down its judgment in *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (Case C-311/18) (*Schrems II*). This judgment has wide-ranging and significant implications for the international transfer of genomic data.

Data protection and genomics

The sharing of genomic data is key to unlocking the benefits of genomics for research and healthcare. The benefits of assembling large cohorts are well-established, enabling data sharing facilitating research into extremely rare events, robust examination of the penetrance of disease, and the study of heterogeneous diseases such as cancer.

The General Data Protection Regulation ("GDPR") is relevant to the sharing of genomic data, as this data can frequently count as personal data and so fall within the scope of the Regulation. Where genomic data constitutes personal data, lawful 'processing' requires a legal basis. If the genomic data constitutes 'special category data' lawful processing will also require an Article 9(2) exception (derogation).

International data transfers

In addition to a legal basis and derogation, lawful transfer of personal data outside the European Economic Area (EEA) requires a legal mechanism for transfer. Post-Brexit transition period, the UK will be outside the EEA and so become a third country. There are three broad varieties of legal mechanism: adequacy decisions, appropriate safeguards, and derogations for specific situations.

Regardless of the legal mechanism picked for transfer, the same standard of 'essential equivalence' applies. In this way, either the jurisdiction must itself provide 'essentially equivalent' protection for the personal data transferred or there must be some further mechanism to provide such protection.

Adequacy between the EU and US is more complex than other jurisdictions. The US *per se* does not have an adequacy decision but has a bespoke system of self-certification, the EU-US Privacy Shield ("Privacy Shield"). Privacy Shield provides a set of principles, a system of oversight, and enforcement mechanisms that provided a basis for transfer.

The other transfer mechanism discussed at length in *Schrems II* is standard contractual clauses (SSCs). SSCs are a form of safeguard to perform international data transfers under Article 46 GDPR. Although the European Commission has adopted sets of these SSCs for use, they must be adopted in their entirety and cannot be modified in any way.

The *Schrems II* judgment

There are three layers to the *Schrems II* judgment: the impact on Privacy Shield, the impact upon SSCs, and wider interpretation of legal mechanisms for transfer more generally, each are considered in turn.

In relation to Privacy Shield, three points are key:

1. The CJEU invalidated the legal underpinnings (Commission Decision 2016/1250) of Privacy Shield (para 201), the Court also invalidating Privacy Shield's predecessor Safe Harbour in 2015 (*Schrems I*). The reasons for doing so center on the primacy of US security and law enforcement powers, as well as the lack of restraint on these powers and redress available to data subjects (para 164-197).
2. It is difficult to see how the differences between US and CJEU positions, made apparent in *Schrems I* and *Schrems II* might be reconciled, with the CJEU intent on upholding 'essential equivalence', the US unwilling to erode their far-reaching security and law enforcement powers - both positions are incompatible, both parties intransigent.
3. The Court declined to keep Privacy Shield alive as an interim measure, the Decision underpinning the agreement is void from the date of the judgment (para 202). This voiding leaves 5,300 EU and US companies in search of a new mechanism for transfer. Even worse, the European data protection regulator the European Data Protection Board (EDPB) has said there is no 'grace period' to adjust to this new situation.

Unfortunately, the judgment also undermined the utility of SSC's, an alternate legal mechanism for transfer:

1. The Court did not invalidate the use of SSCs generally. However, it did interpret SSCs in such a way that will make them difficult to rely upon.
2. The CJEU confirmed that it is not enough to rely upon SSCs alone but controllers, rather than the Court, must 'verify whether the law of the third country of destination ensures adequate protection under EU law' (paras 130, 134). In practice, this means controllers have to conduct 'mini adequacy decisions', examining how the legal regime of that jurisdiction might uphold or undermine the SSC in question.
3. Where a jurisdiction fails to provide sufficient level of protection, the Court recommends using 'other clauses and additional safeguards' (para 132). This is nonsensical - if a jurisdiction provides insufficient protection for standard *contractual* clauses, the addition of more contractual clauses adds little.
4. The CJEU notes that SSCs do not stand alone but might be used alongside other 'supplementary measures' (para 133). However, the Court and the EDPB have thus far failed to clarify what these measures might include.

In short, the CJEU has made it clear that SSCs may in principle be relied upon to facilitate international data transfers but have not clarified how controllers might meet the high bar the Court has now set.

Finally, *Schrems II* primarily considers SSCs, yet the interpretation also impacts upon other safeguards for international data transfer. For instance, the requirement to evaluate SSCs in the context of their jurisdiction also applies to safeguards such as instruments between public authorities, binding corporate rules, codes of conduct, and certification mechanisms. If SSCs fail because a jurisdiction lacks background protections, the same considerations would likely apply to other safeguards.

What does this mean for genomics?

Schrems II is a blow to many who wish to transfer personal data between the EU and US, including the sharing of genomic data. The good news is that not all EU-US transfers of genomic data rely upon Privacy Shield nor use SSCs. Of course, this also makes alternative safeguards (e.g. codes of conduct) more attractive. However, these mechanisms will also be impacted by the wider interpretation of *Schrems II*. Taken together, there are few appealing options to give effect to international data transfers, this is made all the more daunting as the UK will be subject to these rules in less than six months.

Additional information

The GDPR and genomic data report (2020) offers a more extensive exploration of genomic data sharing under the GDPR.

Contact: intelligence@phgfoundation.org

PHG Foundation is a health policy think tank with a special focus on how genomics and other emerging health technologies can provide more effective, personalised healthcare