GDPR and BREXIT

What researchers need to know

Mark Phillips, Information Security at GIDE UK

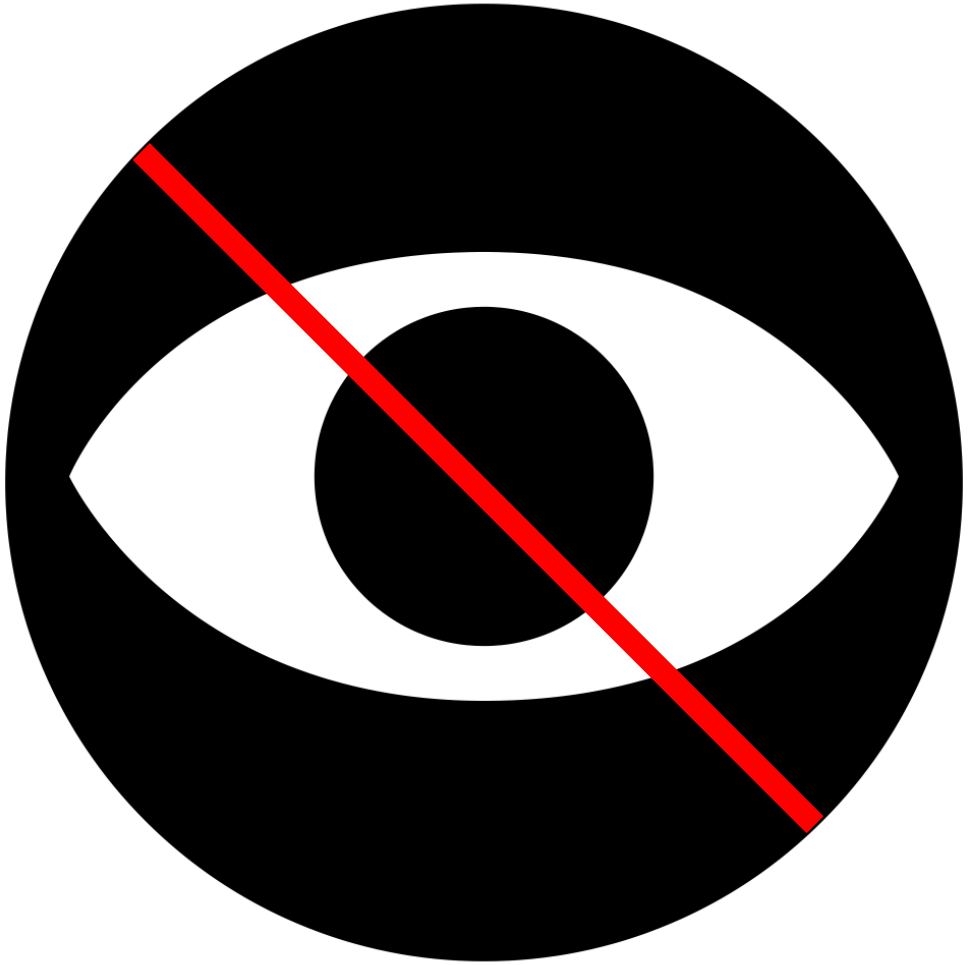
mark.phillips@gide.net

Core principal

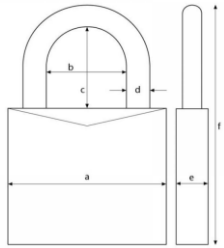
"The protection of natural persons in relation to the processing of personal data is a fundamental right."

In the EU – to which the UK no longer belongs – the sanctity of personal information is fundamental among the rights of human beings and is crystallised as such in the General Data Protection Regulation (GDPR)

It is the perfect allegory for how some of us conceive our existence in the digital age.



40 years in the making



- 1980 OECD's 7 data protection principles (non-binding)
- 1995 EU Data Protection Directive
- 1998 UK Data Protection Act
- 2000 Safe Harbour Privacy Principles
- 2013 Schrems I
- 2015 Safe Harbour deemed invalid by CJEU
- 2016 EU-US Privacy Shield introduced
- 2018 General Data Protection Regulation (GDPR) introduced
- 2018/19 Schrems II
- 2020 Privacy Shield struck down by CJEU
- 2021 Brexit

Privacy is winning

- 2013: Max Schrems challenged Facebook's data processing in light of US Patriot Act/NSA's pre-eminence over personal data

Safe Harbour ruled invalid

- EU-US Privacy Shield replaced it with 'stronger obligations', limitations on and oversight of 'generalised access' by US authorities and an Ombudsperson.
- 2018: 'Data Protection Commissioner v Facebook and Maximillian Schrems' (a.k.a. Schrems II) referred to CJEU as GDPR non-compliant

EU-US Privacy Shield is struck down

General Data Protection Regulation

First conceived in 2012, adopted in 2016 and applied as law on 25/05/2018, the GDPR puts the individual at the front and centre of privacy legislation while the articles and recitals it enshrines go further and harder than all of its predecessors:

- The protection of natural persons in relation to the processing of personal data is a fundamental right. (Recital 1)
- The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should…respect their fundamental rights and freedoms, in particular their right to the protection of personal data. (Recital 2)
- The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must…be balanced against other fundamental rights, in accordance with the principle of proportionality. (Recital 4)

The bottom line:

"EU standards of data protection must travel with personal data when it goes overseas."

How does that work after Brexit?

Adequacy *vs* Sovereignty:

For ‘third countries’ (non-EU) to freely exchange personal data, they must be deemed ‘adequate’ by the European Commission

“…where the Commission has decided that the third country…ensures an adequate level of protection…Such a transfer shall not require any specific authorisation.”

12 countries fulfil this requirement:
Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey New Zealand Switzerland and Uruguay

Adequate chickens…

Sovereign chicken…

The cleft stick

Sovereignty has bought us the right to change our rules, but in doing so it may be at a cost to the adequacy we require.

Meanwhile, having left the EU, and the transition period having expired, the UK is NOT deemed adequate for the moment.

Lessons from America

‘Safe Harbor’ – a fig leaf for the Patriot Act – was brought down by Max Schrems (though it would probably never have met the requirements of GDPR)

The ‘Privacy Shield’ took over, but on January 25 2017, Donald Trump blew it up with Executive Order 13768 Implicated in the Schrems II case, and set against GDPR, it ended the ‘adequacy’ of Privacy Shield

In the UK, our own Investigatory Powers Act 2016 has the potential to undermine our claim to adequacy in the same way

Further (sovereign) divergence post-Brexit, to accommodate the US Cloud Act for example, could further erode this situation.

So, what now?

We’ve left the EU. Transition is over. The UK is a ‘third country’.

How do we run things?

Transfer Scenarios

- Domestic transfers: subject to ‘UK GDPR’ (Data Protection Act 2018), no additional requirements
- Transfers **to** third countries (e.g. USA): subject to UK GDPR, (but note Schrems II and ‘additional safeguards’)
- Transfers **to** EU: no change as already deemed adequate
- Transfers **from** EU received before 01/01/2021: subject to EU GDPR as of 31/12/2020 (‘Frozen GDPR’)
- Transfers **from** EU received from 01/01/2021: new requirements.

The good news…

- The EU/UK Trade and Cooperation Agreement (TCA, the 'big document') allows for an initial '**grace period**' of 4 months (to 01/05/2021) where data transfers can continue as before
- In the absence of an adequacy agreement, and providing the UK does not materially change its data protection regime, this can be extended for a further 2 months (to 01/07/2021)

Phew. But…

- The ICO suggests this time be used to explore contingencies in the event of no adequacy agreement

The ‘Contingencies’

Following the grace period, unless an adequacy decision has been reached, transfers of personal data from the EU to the UK will become a ‘restricted transfer’ requiring extra administration:

1. Registering with a Supervisory Authority/Lead Supervisory Authority
2. Appointing an EU Representative
3. Standard Contractual Clauses
4. Binding Corporate Rules
5. The Data Protection Officer (DPO)
6. Securing data in transit
7. Securing data at rest

Data storage, post Schrems II

- US can unilaterally seize data from:

"…all electronic communication service or remote computing service providers that are subject to U.S. jurisdiction..."

- Which includes any foreign entity with an office or subsidiary in the US
- Fundamentally incompatible with GDPR
- CJEU continues to recognise the use of SCCs, subject to risk assessment, but with 'additional safeguards'.

Additional safeguards?

Going in hard: The German state of Baden-Württemberg were first out of the trap with specifics. They were:

- Encryption for which “only the data exporter has the key” and which “cannot be broken by U.S. intelligence services”
- Anonymization, or Pseudonymization, where “only the data exporter can re-identify the data”

Might this be the future of data transfer, post-Brexit?

About GIDE

For over 25 years we've worked with government, LAs and some of the largest social and market research organisations. We've securely delivered tens of thousands of data collection and reporting projects, from very small to some of the largest and most complex around.
Perhaps you've heard of the School Performance Tables? Or the national Pupil Eligibility Checking service? Or maybe the UK Resilience Capability Survey? Yes, we did those.
Government trusts us. Industry trusts us.
You can trust us too.

If you'd like to discuss your project with us contact robert@gide.net
If you have any questions about GDPR contact mark.phillips@gide.net

www.gide.uk