


BREXIT – DATA PROTECTION IMPLICATIONS FOR THE UK

James Castro-Edwards, Partner
jcastro-edwards@wedlakebell.com

 @jcastroedwards

 **LinkedIn**



BREXIT – DATA PROTECTION IMPLICATIONS FOR THE UK



Overview

1. Data protection legislation in the UK
2. The Information Commissioner's Office (ICO)
3. Data protection implications of Brexit
4. Possible outcomes
5. What this means in practice

DATA PROTECTION LEGISLATION IN THE UK

The GDPR, DPA 2018 and PECR

1. The UK adopted the GDPR on 25th May 2018
2. In the UK, the GDPR is supplemented by the Data Protection Act 2018
3. The GDPR and DPA 2018 replaced the Data Protection Act 1998, which implemented Directive 95/46/EC into law in the UK
4. Unsolicited, direct marketing is regulated by The Privacy and Electronic Communications (EC Directive) Regulations 2003 (**PECR**), which implement Directive 2002/58/EC

THE INFORMATION COMMISSIONER'S OFFICE (ICO)

The ICO – a very active regulator

1. The GDPR, DPA 2018 and PECR are enforced by the Information Commissioner, acting through her office, the ICO
2. The Information Commissioner, Elizabeth Denham, was previously the Information and Privacy Commissioner for British Columbia, Canada and Assistant Privacy Commissioner of Canada: a professional data protection commissioner
3. The ICO announced an intention to hire 200 new staff (a 40% increase) to police compliance, bringing the ICO to a target staff of around 700
4. Enhanced pay arrangements for ICO staff to prevent poaching

THE INFORMATION COMMISSIONER'S OFFICE (ICO)



ICO enforcement activities since Sep 2017:

1. 18 enforcement notices
2. 8 undertakings accepted
3. 33 monetary penalties
4. Approx. £5,000,000 issued in fines

THE INFORMATION COMMISSIONER'S OFFICE (ICO)

The ICO – what gets controllers into trouble?

- Equifax: Fined **£500,000** for failure to protect personal data 15m UK citizens (Sep 18)
- Everything DM Ltd: **£60,000** for sending email marketing without consent (Sep 18)
- Lifecycle Marketing (Mother and Baby) **£140,000** for Illegally collecting and selling personal information belonging to > 1M people. (Aug 18)
- Independent Inquiry into Child Sexual Abuse **£200,000** for Revealing identities of abuse victims in mass email (security measures). (July 18)
- Our Vault Ltd – fined **£70,000** – for making 55,534 unsolicited marketing calls to people who had registered with the Telephone Preference Service (TPS) (June 18)

THE INFORMATION COMMISSIONER'S OFFICE (ICO)

The ICO – what gets controllers into trouble?

- British Telecommunications: **£77,000** fine for sending 5M nuisance emails (June 18)
- Gloucestershire Police: **£80,000** for revealing information about abuse victims in a mass email (security measures) (June 18)
- The British & Foreign Bible Society c/o the Bible Society: **£100,000** for security breach as a result of a cyber attack. (June 18)
- Bayswater medical centre: **£35,000** for physical security breach (May 18)
- University of Greenwich: **£120,000** for a security breach affecting 20,000 (May 18)
- Yahoo! UK Services Ltd: **£250,000** – network security failings (May 18)

DATA PROTECTION IMPLICATIONS OF BREXIT

Will the GDPR still apply in the UK, post-Brexit?

1. The British Government and the ICO have consistently stated that the GDPR will continue to apply, post-Brexit
2. More recently, the UK Government made the following statement:
‘the Data Protection Act 2018 would remain in place and the EU Withdrawal Act would incorporate the GDPR into UK law to sit alongside it’

The GDPR is here to stay, and the ICO will actively enforce it!

DATA PROTECTION IMPLICATIONS OF BREXIT

What will change, post Brexit?

1. In the absence of a deal to the contrary, the UK will become a ‘third country’
2. EU Member States are prohibited from transferring personal data to third countries that do not guarantee adequate protection
3. Unless the European Commission makes an adequacy decision in favour of the UK, controllers and processors in Member States will be prohibited from transferring personal data to the UK, unless they take other measures

POSSIBLE OUTCOMES

The three possible outcomes are:

1. **No deal** – the UK becomes a 3rd country
2. **Adequacy decision** – the UK is recognised as an approved country
3. **Enhanced adequacy decision** – the UK is recognised as an approved country and participates in the European Data Protection Board.

POSSIBLE OUTCOMES

1. No Deal

- The UK becomes a 3rd country
- EU Controllers will *prima facie* be prohibited from transferring personal data to the UK – including between group companies
- But EU data transfer solutions would still be effective:
 - EU Model Clauses
 - Binding Corporate Rules (BCR)
 - Approved codes of conduct (e.g. Privacy Shield) – none exist yet, and may be problematic!
- UK-EU transfers unaffected
- In practice, this would be like doing business with the US

POSSIBLE OUTCOMES

2. Adequacy Decision

- The UK becomes a 3rd country – but approved as providing adequate protection
- EU Controllers would be able to freely transfer personal data to the UK (& vice versa)
- But ICO / EU DPA rules may diverge over time
- ICO would be outside the ‘one stop shop’ mechanism – i.e. controllers will need to pay the ICO fee
- Despite adopting the GDPR, and ‘complete convergence’ an adequacy decision is *not* a forgone conclusion
- An adequacy decision is threatened by EU/UK relations, and by the controversial UK Investigatory Powers Act 2016 (aka ‘The Snoopers’ Charter’)
- The EU has not given a timetable for an adequacy assessment

POSSIBLE OUTCOMES



3. Enhanced Adequacy Decision

- The UK becomes a 3rd country – but approved as providing adequate protection
- EU Controllers would be able to freely transfer personal data to the UK
- The ICO would participate with EU supervisory authorities, so limited UK / EU divergence
- If successful, the ‘enhanced adequacy decision’ would mean business as usual
- So far, this proposal has met with resistance from the European Commission

WHAT THIS MEANS IN PRACTICE

Practical compliance for European companies doing business with the UK

1. The GDPR, DPA 2018 and PECR are actively enforced by the ICO – the UK is not a ‘soft touch’
2. Post-Brexit, data transfer solutions may be necessary – depending on the UK/EU arrangement - the UK govt. recommends Model Clauses and BCRs; other solutions, such as codes of conduct may become available in the future
3. Not just data transfers – UK subsidiaries must comply with GDPR principles

WHAT THIS MEANS IN PRACTICE

Practical compliance for European companies doing business with the UK

1. Breach notification processes must be robust, and effective
2. Organisations must be able to deal with data subjects' requests to exercise their rights
3. Controllers must document sharing arrangements with processors and joint controllers
4. DPIAs must be carried out for 'high risk' processing activities
5. Controllers must have compliance documentation in place

BREXIT – DATA PROTECTION IMPLICATIONS FOR THE UK


Questions?

BREXIT – DATA PROTECTION IMPLICATIONS FOR THE UK

James Castro-Edwards, Partner
jcastro-edwards@wedlakebell.com

 @jcastroedwards

 **LinkedIn**

