LEWIS SILKIN

8th February 2019

No deal Brexit and Data Protection

What UK businesses need to know and how you should prepare

With the Brexit D-day of 29 March looming, organisations have asked us to help prepare a Brexit Data Response Plan in case of a potential no deal Brexit. Building on the ICO and DCMS Guidance Notes*, we provide below some data protection considerations and sensible actions to take to ensure that your organisation's data governance is ready.

What will not change?

- **General Data Protection Regulation 2016/679 (GDPR):** Businesses should continue to maintain compliance with GDPR standards, as it will still be applicable through the UK GDPR.
- **Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) and Network and Information Systems Regulations 2018 (NIS)**: Both PECR and NIS will continue to apply.
- **Data transfers from the UK to the EEA:** The UK will still recognise transitionally all EU/EEA countries and Gibraltar as 'adequate', all EU adequacy decisions in relation to third countries, and the EU model clauses (SCCs), as providing 'adequate' protection for data flows out of the UK.
- **Data transfers from the UK to the US:** The UK will still recognise the EU-US Privacy Shield, provided that US organisations comply with new guidance set out on the US Government's Privacy Shield website, which requires amending public commitments applicable to transfers of personal data from the UK.
- **Binding Corporate Rules (BCRs):** There is continued recognition by the ICO of BCRs that have been authorised before Brexit.

What will change?

- **Data transfers from the EEA to the UK:** The UK will be considered a "third country" by the EU and no 'adequacy' decision by the EU Commission will apply. Data transfers from the EU to the UK will need to be subject to the same 'appropriate safeguards' (e.g. the use of SCCs) that apply to other third countries.
- **Appointing an EU or a UK representative:** Controllers or processors based outside or inside the EEA may need to appoint a representative in the UK if they offer goods or services to, or monitor the behaviour of, UK individuals. Equally, any UK-based controller or processor without a presence in the EEA, targeting EEA individuals, may need to appoint an EU representative.
- **Binding Corporate Rules (BCRs):** Existing BCRs certified by the ICO may not be recognised by the EU supervisory authorities, affecting data transfers from the EEA to the UK.
- **One-Stop Shop and Lead Supervisory Authority (LSA):** The ICO can no longer act as a LSA. UK-only based organisations, or those only present in the UK plus one EU country, may no longer have access to the one-stop-shop mechanism.
- **Organisational awareness:** Company boards need to empower the legal team, the compliance team and/or DPOs to ensure that plans and budgets are allocated to the Brexit Data Response Plan.

***ICO Guidance**: https://ico.org.uk/for-organisations/data-protection-and-brexit/data-protection-if-there-s-no-brexit-deal/;
UK Government – DCMS Technical Note: https://www.gov.uk/government/publications/data-protection-law-eu-exit/amendments-to-uk-data-protection-law-in-the-event-the-uk-leaves-the-eu-without-a-deal-on-29-march-2019

Find out more

twitter.com/LewisSilkin
linkedin.com/company/lewis-silkin

For more information, please contact:

Dr. Nathalie Moreno
Partner

+44 (0)20 7074 8461
nathalie.moreno@lewissilkin.com