Brexit Data Protection Checklist	
Which data protection regime(s) will apply to your organisation?	• The UK will have its own data protection regime, separate from, but closely mirroring, the GDPR (at least in the short term). The UK regime will consist of the UK GDPR and the (amended) Data Protection Act 2018. • The GDPR and the UK data protection regime both have extra-territorial scope. Therefore, organisations with establishments in both the EEA and the UK, or which offer goods or services to, or monitor the behaviour of, individuals in the EEA and UK, will be subject to both the GDPR and the UK regime. • Organisations should seek to determine which regime(s) they are subject to, and in relation to which of their data processing activities. This mapping exercise will become increasingly important if the UK regime diverges from the GDPR over time.
Which data protection supervisory authorities will supervise your organisation?	• UK-based organisations that are subject only to the UK data protection regime will be supervised solely by the Information Commissioner's Office (ICO). • Organisations that are subject to both the GDPR and the UK regime, and that previously considered the ICO to be their lead data protection supervisory authority, will need to identify which (if any) EEA supervisory new lead authority in the EEA. Organisations will also need to deal with the ICO for their UK data processing. • Organisations under the supervision of the ICO and relevant EEA authorities should consider their strategy in the event they face parallel enforcement actions/fines in the UK and the EEA (which could potentially be across multiple EEA jurisdictions if a lead authority/the GDPR 'one-stop-shop' mechanism is not available).
Does your organisation need to appoint a UK and/or EEA representative?	**Data Protection Representatives** • EU Representative: The GDPR requires organisations that are subject to the GDPR but not established in the EEA to appoint an EEA representative. From 1 January 2021, this requirement will apply to UK organisations that are subject to the GDPR, but do not have an establishment in the EEA. • UK Representative: The UK regime mirrors the GDPR's representative requirements, therefore, organisations that are subject to the UK data protection regime but not established in the UK will be required to appoint a UK representative.
	Network and Information Security Directive (NIS) Representatives • EU NIS Representative: The NIS Directive requires relevant digital service providers that are offering services in the EEA and subject to NIS, but with head offices outside of the EEA, to appoint a representative. From 1 January 2021, this requirement will apply to UK head office digital service providers offering services in the EEA. Such UK digital service providers will need to appoint a NIS representative in one of the EU Member States where services

	are offered (following the national laws implementing the NIS Directive in that country). • UK NIS Representative: The UK NIS Regulations mirror the NIS Directive's representative requirements. Therefore, digital service providers with their head office in the EEA or elsewhere outside the UK, providing digital services in the UK, will be required to appoint a UK NIS representative (and confirm this in writing following the ICO representative registration process).
Does your organisation need to change/ extend its Data Protection Officer (DPO) structure?	• The GDPR requirement to appoint a DPO is maintained under the UK data protection regime. • Organisations may rely on their existing DPO appointment for both GDPR and UK regime purposes, whether that DPO is in the EEA or the UK, provided the DPO requirements can be met in relation to both their EEA and UK establishments (e.g., accessibility to individuals and authorities, and appropriate knowledge and resources).
Does your organisation need to update its personal data transfer mechanisms?	**EEA to UK** • The data transfer grace period under the Trade Agreement allows personal data to be transferred from the EU to the UK as if the UK has not become a third country on 1 January 2021 (i.e., no GDPR data transfer mechanism is required), for at least four months, to be extended by a further 2 months unless either the EU or the UK objects. The grace period arrangements are conditional upon the UK maintaining its 'Brexit transition period' data protection regime (i.e. the data protection laws in place on 31 December 2020) during the grace period. • If the Commission adopts a UK adequacy decision during the grace period, the grace period will end, and organisations can rely on that adequacy decision to permit EEA to UK personal data transfers. • If the Commission does not adopt a UK adequacy decision during the grace period, the UK will be considered a third country for personal data transfers at the end of the grace period. In these circumstances, organisations should ensure that they have an effective data transfer mechanism in place for data transfers from the EEA to the UK, including any onwards transfers. • The most frequently used GDPR data transfer mechanism is the standard contractual clauses (SCCs). While the SCCs are likely to remain the most feasible option for the majority of data transfers, the Court of Justice of the European Union's (CJEU) *Schrems II* decision and the subsequent draft Recommendations from the European Data Protection Board have introduced several challenges to their use in practice. Broadly, organisations are required to carry out risk assessments for each data transfer, and to put in place additional safeguards to adequately protect personal data if required. These requirements apply to all data transfers including those to the UK. • Additionally, the European Commission has recently published a draft set of updated standard contractual clauses (the New SCCs), which substantially update the SCCs terms. Once finalised and approved, the New SCCs will replace the SCCs for personal data transfers, though organisations will benefit from a 12-month grace period to enter into the New SCCs. It is hoped that the New SCCs will be approved by the end of the data transfer grace period

	under the Trade Agreement, in the event that no UK adequacy decision is adopted by the Commission during that grace period - In these circumstances, if the New SCCs are *not* approved by the end of the data transfer grace period, organisations looking to rely on SCCs for transfers to the UK should factor in the requirement to replace those SCCs with the New SCCs within the proposed 12-month New SCCs grace period.
	UK to EEA and rest of the world • The UK will transitionally recognise all EEA member states, Gibraltar, all EU and EEA institutions, and all existing adequacy decisions as providing an adequate level of protection for personal data transfer purposes under the UK regime. This means that data transfer mechanisms will not be required for such transfers. The UK will also recognise existing SCCs and Binding Corporate Rules (BCRs).
Does your organisation need to update its Binding Corporate Rules (BCRs)?	**UK-approved BCRs** • Organisations with BCRs approved by the ICO under the GDPR will require a new approval from a new BCR lead supervisory authority in the EEA, in order for their BCRs to continue to provide a valid GDPR data transfer mechanism. Organisations will also need a parallel set of BCRs for the UK. • The UK regime maintains the BCR mechanism, and the ICO may approve domestic BCRs for data export solely from the UK.
	EEA approved BCRs • The ICO will continue to recognise any existing EEA-approved BCRs as valid data export mechanisms from the UK. Organisations are required to take several steps to maintain their BCRs, including creating a parallel set of BCRs for the UK with a separate intra-group agreement/ binding instrument.
What updates should your organisation make to its data protection documentation?	**Data processing agreements/terms; data transfer agreements** • Organisations should review and update their contractual data protection terms to reflect the distinction between the European and UK data protection regimes (if relevant). Key elements likely to require amendment include data protection definitions (e.g., 'Applicable Data Protection Laws', 'Third Country', etc.); references to GDPR articles; and data transfer/data export wording.

Privacy policies

Privacy policies may need to be updated to reflect:

- Updated references to applicable legal regimes and supervisory authorities
- Applicable changes to data processing grounds (for example, a UK company may no longer be able to rely on compliance with an EU or EU member state law as a ground for processing, and national law grounds for processing special categories of personal data may no longer be available)
- New data transfers mechanisms for any transfers from the EEA to the UK, and updated information about any transfers from the UK to the EEA
- Details of any newly appointed UK and/ or EU representatives
- Any updated DPO details
- Any changes to BCR details

Data Protection Impact Assessments (DPIAs); records of processing

- Organisations should review their DPIAs (and Legitimate Impact Assessments) and records of processing, updating such documentation if required, to reflect any changes to data export arrangements and data processing grounds.