ashurst

GDPR in Financial Services: 2022 Regulatory Hotspots

30 MARCH 2022

GDPR in Financial Services: 2022 Regulatory Hotspots

Rhiannon Webster
Partner and Head of Data Protection Practice

T +44 20 7859 3070
Rhiannon.Webster@ashurst.com

Jake Green
Practice Global Co-Head, Financial Regulatory

T +44 20 7859 1034
Jake.Green@ashurst.com

Shehana Cameron-Perera
Senior Associate, Digital Economy

T +44 20 7859 2768
Shehana.Cameron-Perera@ashurst.com

Please send questions direct to our speakers via the chat box

"Advice on governance has been absolutely outstanding; they've been extremely critical to our success."

CHAMBERS & PARTNERS UK

ashurst

Regulatory Hotspots

Privacy laws in 80% of countries worldwide

UK and EU GDPR

Schrems II – overhaul of approach to data transfers

EU and US announce European Commission and the United States announce a new Trans-Atlantic Data Privacy Framework

Bank fined by Swedish DPA for violation of GDPR transparency requirements

H&M fined €35.25 million following technical error which resulted in network drive and medical records being fully accessible internally

WhatsApp fined €225 million by DPC for lack of transparency

Google fined €60 million by CNIL for placing advertising cookies on users' computers without consent

Activist Austrian privacy group are conducting cookie sweeps

Austria and France find Google Analytics' transfer of data to the US illegal

GDPR in Financial Services: 2022 Regulatory Hotspots

AGENDA

1. The consequences of Brexit on data protection compliance

2. International transfers post Schrems II

3. Stress testing your data breach response procedures

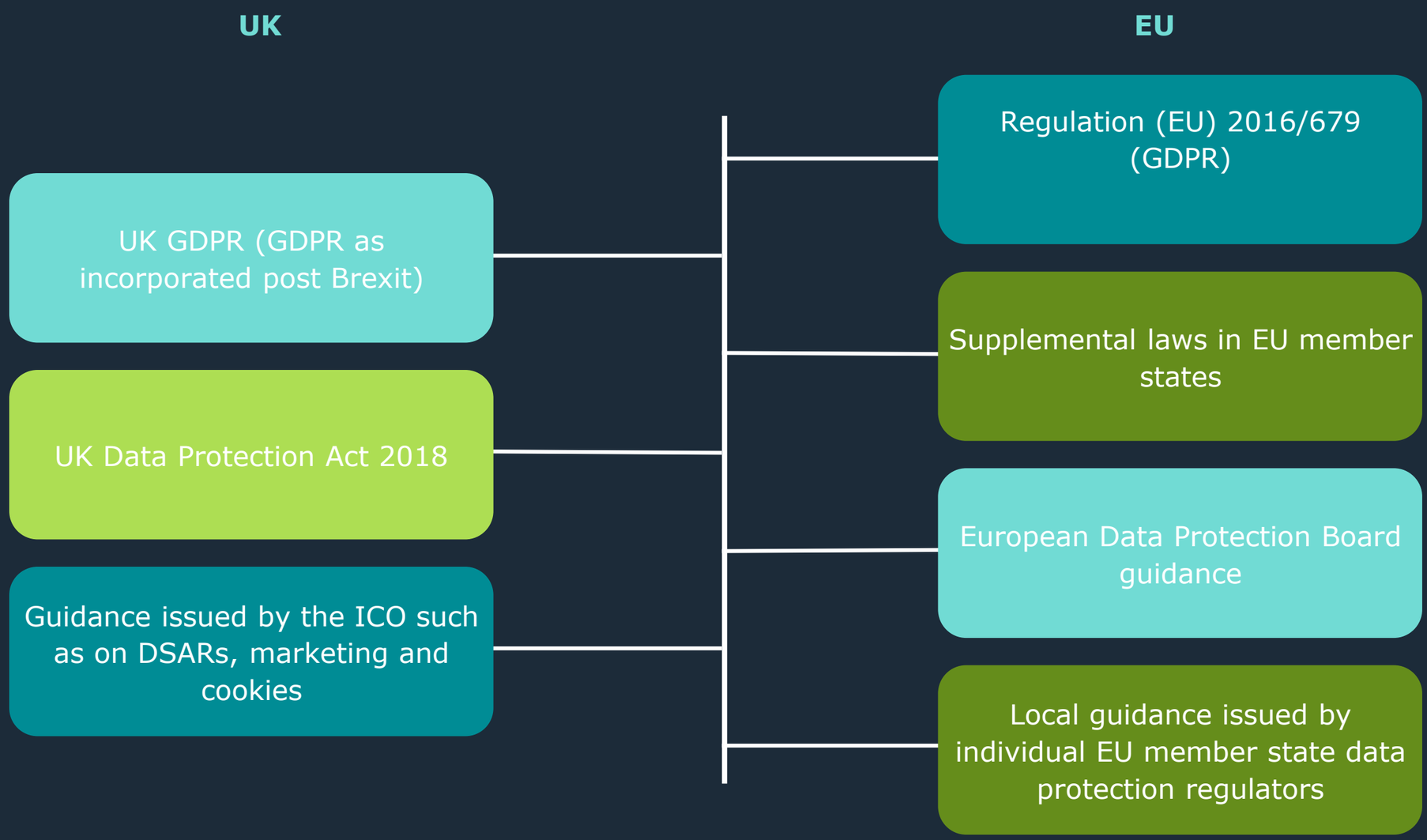
Please send questions direct to our speakers via the chat box

ashurst

CONSEQUENCES OF BREXIT ON DATA PROTECTION COMPLIANCE

ashurst

Legislative Framework in the UK and the EU



Both UK and EU GDPRs have extra territorial scope i.e. it can apply to organisations based outside the EU/UK that do not have an establishment (such as offices/branches) in the EU/UK.

Is the UK Data Protection Regime going to fundamentally change?

In September 2021, the UK's Department for Digital, Culture, Media and Sport (DCMS) launched a consultation on the future of UK data protection law, proposing changes to the current legislation including:

- Accountability with flexibility – "Privacy Management Regime"
- Removal of mandatory designation of DPOs
- Removal of requirement to carry out DPIA
- Data breach reporting only if "material"
- Re-introduce a fee for subject access requests
- Legitimate interests "whitelist"

How likely is a radical overhaul of the UK data protection regime?

Brexit Freedoms Bill means that making changes to EU retained law such as the UK GDPR can be quick and without much Parliamentary scrutiny

INTERNATIONAL TRANSFERS POST SCHREMS II

ashurst

Data Transfers – will your organisation be affected?

Making a transfer to a group company based overseas for reporting purposes or a transfer to a US parent company

Simply allowing remote access into UK systems from service providers based overseas

What is a data transfer?

- Actual disclosure
- Hosting
- Making personal data available eg remote access/ granting access

Transfer of client files to or from clients in third countries

An external transfer of employee data to a third party such as Workday hosted in the US or payroll or employee benefit providers in third countries

Allowing UK and EU based service providers to use systems or sub processors based overseas

ashurst

Schrems II: What happened next?

16 July 2020

CJEU Issues judgement on Schrems II

23 July 2020

EDPB issues FAQ guidance on the Schrems II decision.

- No grace period: transfers under the privacy shield should cease immediately
- Principles apply to any other Third Country transfer, not just the U.S.

10 November 2020

EDPB adopts Recommendations 02/2020 on the EEG for surveillance measures

10 November 2020

EDPB issues version 1.0 of the recommendations for supplementary measures

11 November 2020

EDPB consultation on version 1.0 of the recommendations for supplementary measures

12 November 2020

EU Commission consultation on new Standard Contractual Clauses issued

2021

4 June 2021

EU Commission adopts the new Standard Contractual Clauses

18 June 2021

The EDPB adopts Recommendations 01/2020 for supplementary measures

2022

21 March 2022

UK IDTA and Addendum are effective

Please send questions direct to our speakers via the chat box

ashurst

Privacy Shield No. 2 – does this change anything?

European Commission

TRANS-ATLANTIC DATA PRIVACY FRAMEWORK

March 2022

The European Commission and the United States reached an agreement in principle for a **Trans-Atlantic Data Privacy Framework.**

Key principles

- Based on the new framework, **data will be able to flow freely and safely** between the EU and participating U.S. companies
- A new set of rules and **binding safeguards to limit access to data** by U.S. intelligence authorities to what is **necessary and proportionate** to protect national security; U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards
- **A new two-tier redress system** to investigate and resolve complaints of Europeans on access of data by U.S. Intelligence authorities, which includes a **Data Protection Review Court**
- **Strong obligations for companies** processing data transferred from the EU, which will continue to include the requirement to self-certify their adherence to the Principles through the U.S. Department of Commerce
- **Specific monitoring and review mechanisms**

Benefits of the deal

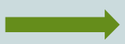
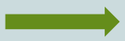
- Adequate protection of Europeans' data transferred to the US, addressing the ruling of the European Court of Justice (*Schrems II*)
- Safe and secure data flows
- Durable and reliable legal basis
- Competitive digital economy and economic cooperation
- Continued data flows underpinning €900 billion in cross-border commerce every year

Next steps: The agreement in principle will now be translated into legal documents. The U.S. commitments will be included in an Executive Order that will form the basis of a draft adequacy decision by the Commission to put in place the new Trans-Atlantic Data Privacy Framework.

Justice and Consumers

ashurst

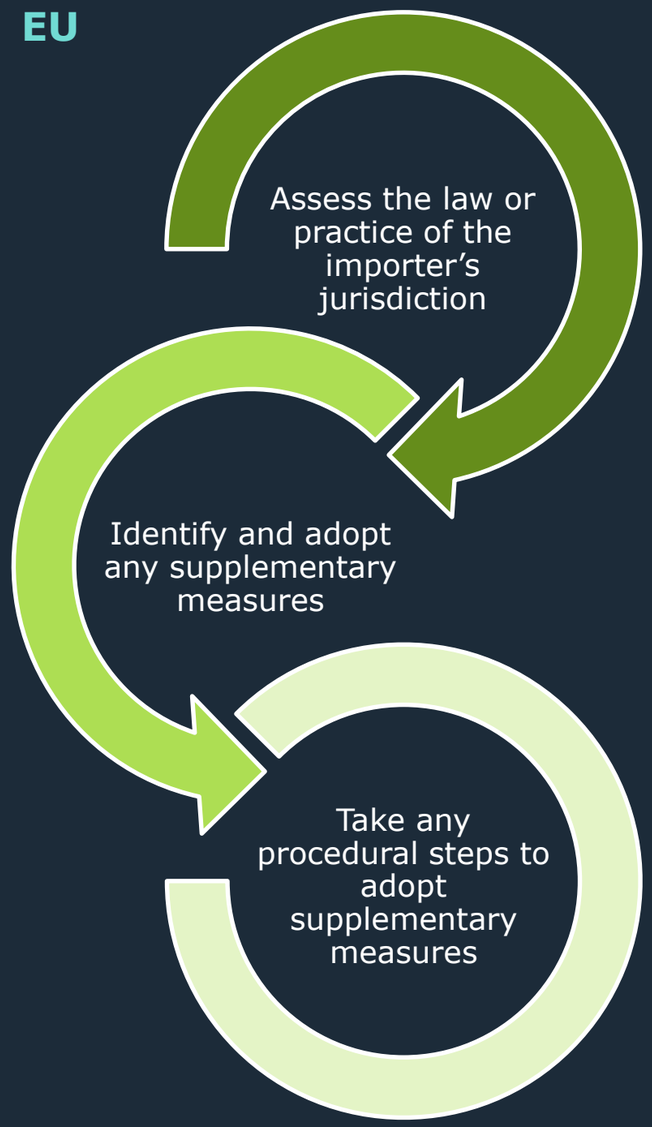
Overview of transfers from the EU and the UK

Jurisdiction of Transfer			Transfer Details
			UK was deemed adequate on 28 June 2021. **No transfer mechanism is required for data to flow.** UK Adequacy decisions include a so-called "sunset clause" – they expire automatically, four years after entry.
			Data can flow freely to EU Member States and other EEA states. **No transfer mechanism is required.**
 		Adequate Countries	Data importer is located in a jurisdiction which has been deemed "adequate" by the EU (the full list is available at Adequacy decisions | European Commission (europa.eu)) or the UK government (as it has the power to make its own adequacy decisions). **No additional transfer mechanism is required.**
 		Third Country	**A transfer mechanism and transfer impact/risk assessment is required**.

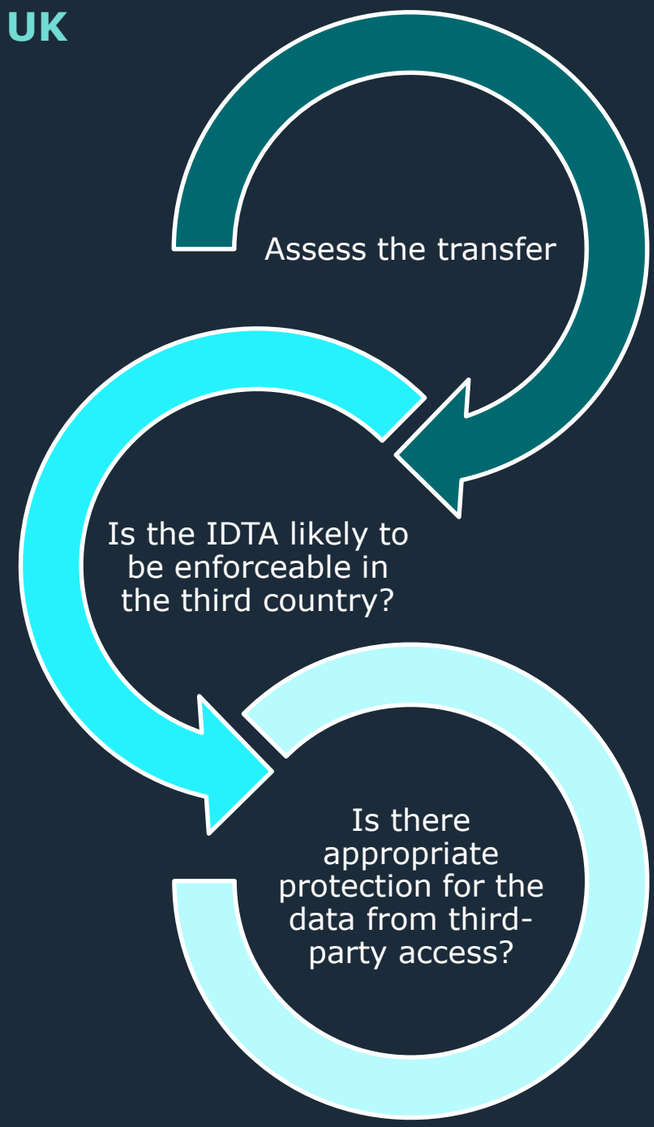
ashurst

EU TIA versus UK TRA

EU



UK



ashurst

UK International Data Transfer Agreement and the EU Standard Contractual Clauses – a Comparison

IDTA	EU SCCS
• Single "one size fits all" data transfer agreement. • Clearer, user friendly. Flexible and conscious of commercial context.	• Modular: Controller to Controller; Controller to Processor; Processor to Sub Processor; Processor to Controller. • Requires "constructing" for your particular scenario.
Anticipates a "linked" commercial agreement (such as a master services agreement or similar) and allows for the incorporation of the terms of that "linked" agreement into the IDTA provided the rights granted under the IDTA are not affected.	No such flexibility – drafting amendments needed
Can be used if a processor transfers personal data to an organisation which is not its instructing controller, or its sub-processor (for example, a processor transferring data to another processor appointed by the instructing controller).	Restricted to the 4 modules listed above

UK International Data Transfer Agreement and the EU Standard Contractual Clauses – a Comparison

IDTA	EU SCCS
Part 2 specifically allows for any additional safeguards/supplementary measures required by Schrems II and the EDPB's associated recommendations on supplementary measures to be separately listed in the IDTA	No such flexibility – drafting amendments needed
Can be used even if the importer is directly subject to the UK GDPR.	Confusion reigns. Recital 7 of the implementing decision for the new EU SCCs states that they may only be used "to the extent that the processing by the importer does not fall within the scope of" the EU GDPR, begging the question of what clauses should be implemented where the importer does fall within the EU GDPR on an extra-territorial basis.
Mandatory Article 28 Clauses not included	Incorporates the Article 28 Clauses

UK Addendum to new EU SCCS

What is it?

- UK Addendum is an "add-on" or "bolt on" to New EU SCCs.
- UK Addendum to the New EU SCCs will:
  - incorporate new EU SCCs; and
  - amend them to ensure compliance with the UK GDPR.

How can it be used?

- Can be used by organisations who have either:
  - have either already entered into the New EU SCCs; or
  - want to use the New EU SCCs because they transfer personal data from both the UK and the EEA.

Practical steps to tackling TIAs/TRAs

ROOT AND BRANCH APPROACH

Root Assessment

- Categorise and group transfers by type of industry and jurisdiction
- This will be a template TIA/TRA for that Categorisation

Branch Assessment

- Each data transfer will then need to be treated as a branch
- The template TIA/TRA should be amended on a case by case basis to reflect the specific details of transfer and data importer

It will be impossible to get the risk to zero. Therefore it is about risk management of the residual risk:

- Have you done everything to eliminate the risk to privacy? E.g. can you pay for a UK/EU data centre?
- Can the process/transfer be stopped? Assess its critical value.
- Self-assess the risk taking into consideration your organisation's risk profile? I.e. are ISCO/key decision makers risk adverse?
- What is the worst case scenario? Are you prepared to take the risk?

Timeframes for remediation

4 June 2021

New EU SCCs were adopted

27 June 2021

New EU SCCs are effective

From 27 September 2021

New EU SCCs must be used for all new transfers or where there are changes to existing transfers.

21 March 2022

UK IDTA and IDTA Addendum are effective

Until 21 September 2022

Can use ICO version of old EU SCCs as long as contract is concluded on or before 21 September 2022 and processing operations remain unchanged (for example, there are no changes to sub-contracting).

However, irrespective of this, we highly advise using UK IDTA/Addendum going forward.

From 21 September 2022

UK IDTA and IDTA Addendum must be used for all new transfers and changes to existing transfers

From 27 December 2022

Old EU SCCs no longer valid. Repapering exercise for EU to be completed.

By 21 March 2024

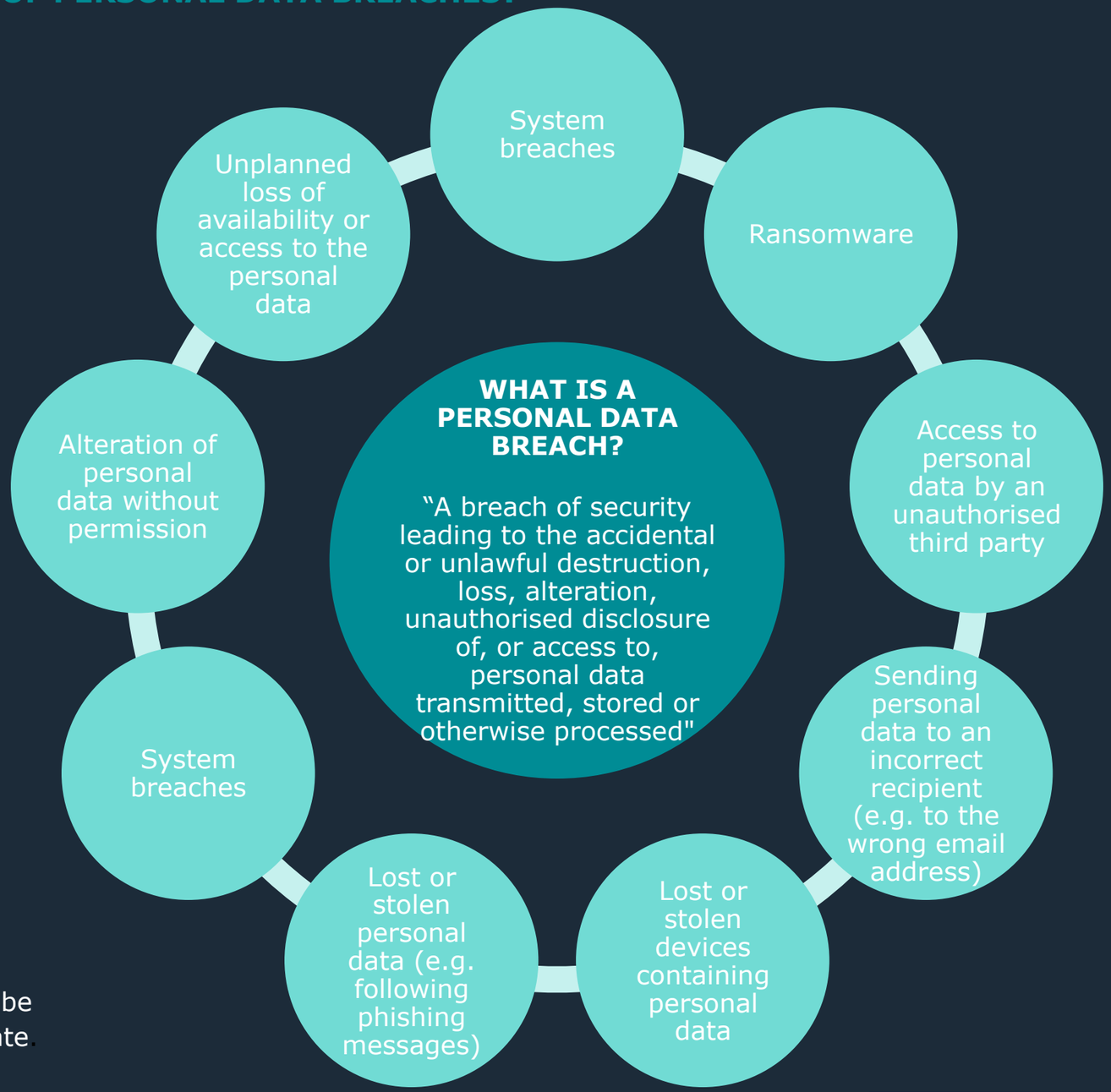
Repaper all existing contracts which incorporated ICO version of old EU SCCs

DATA BREACHES

ashurst

What is a personal data breach?

WHAT ARE EXAMPLES OF PERSONAL DATA BREACHES?



The above examples can be categorised as being: **confidentiality breaches, integrity breaches or availability breaches.**

Personal data breaches can be both accidental and deliberate.

ashurst

Controller's assessment of whether to notify

You must establish the likelihood (of the damage occurring) and severity of the impact (of the damage) and European guidance recommends taking into account:

Type of breach: e.g. where medical data has been disclosed to unauthorised parties, this will likely have different consequences to where an individual's medical details have been lost, and are no longer available.

Nature, sensitivity and volume of personal data: generally, the more sensitive the data, the higher the risk of harm. Always consider the wider context. Combinations of personal data affected are also typically more sensitive than a single piece of personal data.

Ease of identification of individuals: consider whether this personal data can be matched with other publicly available information or whether the personal data automatically directly identify particular individuals.

Severity of consequences for individuals: e.g. could the personal data cause psychological distress/humiliation? Who is the personal data now in the hands of? Is it a trusted organisation who has provided assurances that they have deleted it?

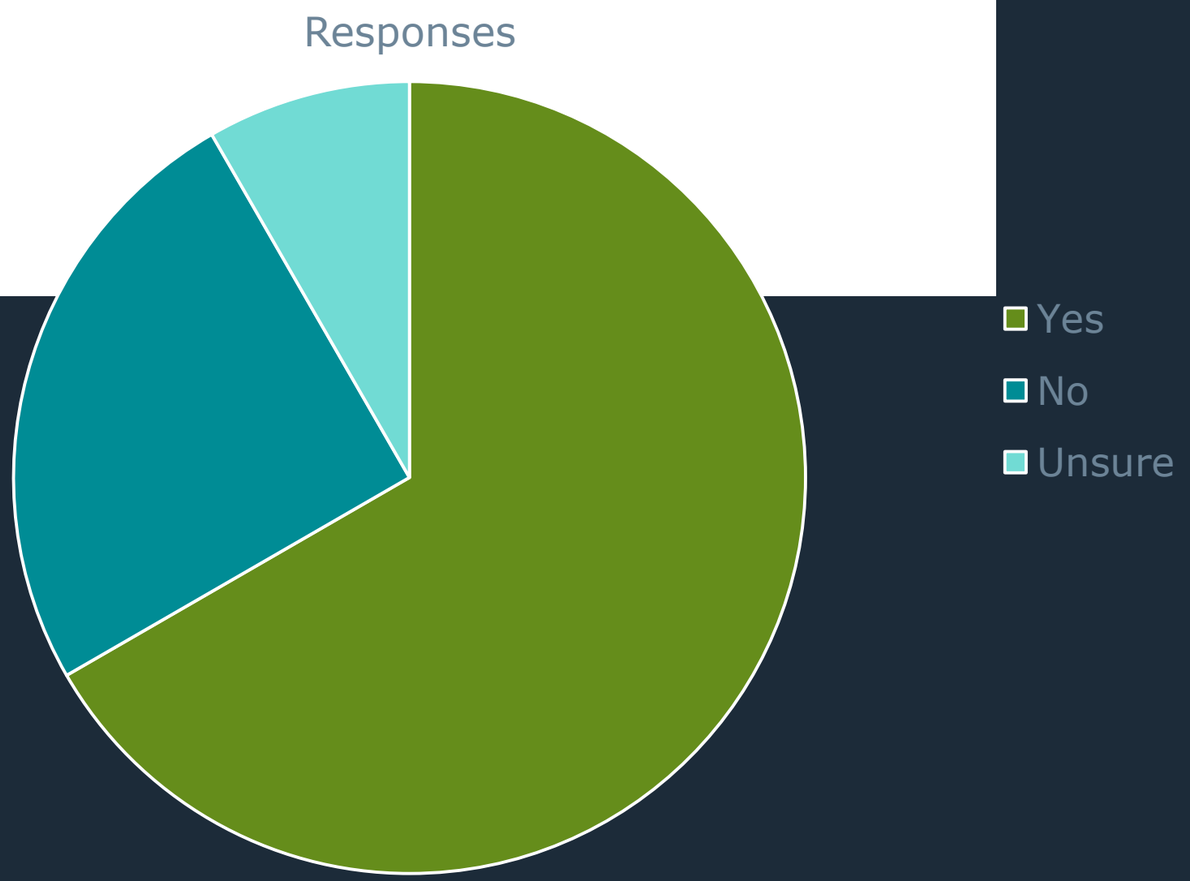
Special characteristics of the individual: does the personal data breach concern children/vulnerable individuals?

Number of affected individuals: generally, the higher the number of individuals affected, the greater the impact of a breach.

Case studies – Scenario One

1. **Scenario One**: It's Friday afternoon and you become aware that there may have been access to your client systems from a threat actor. You have over 2,000 clients listed on your CRM system made up of corporate clients and retail clients. It becomes clear that names and email addresses of all such clients have been accessed by the threat actor. Do you notify the ICO and/or data subjects?

- ◯ Yes
- ◯ No
- ◯ Unsure



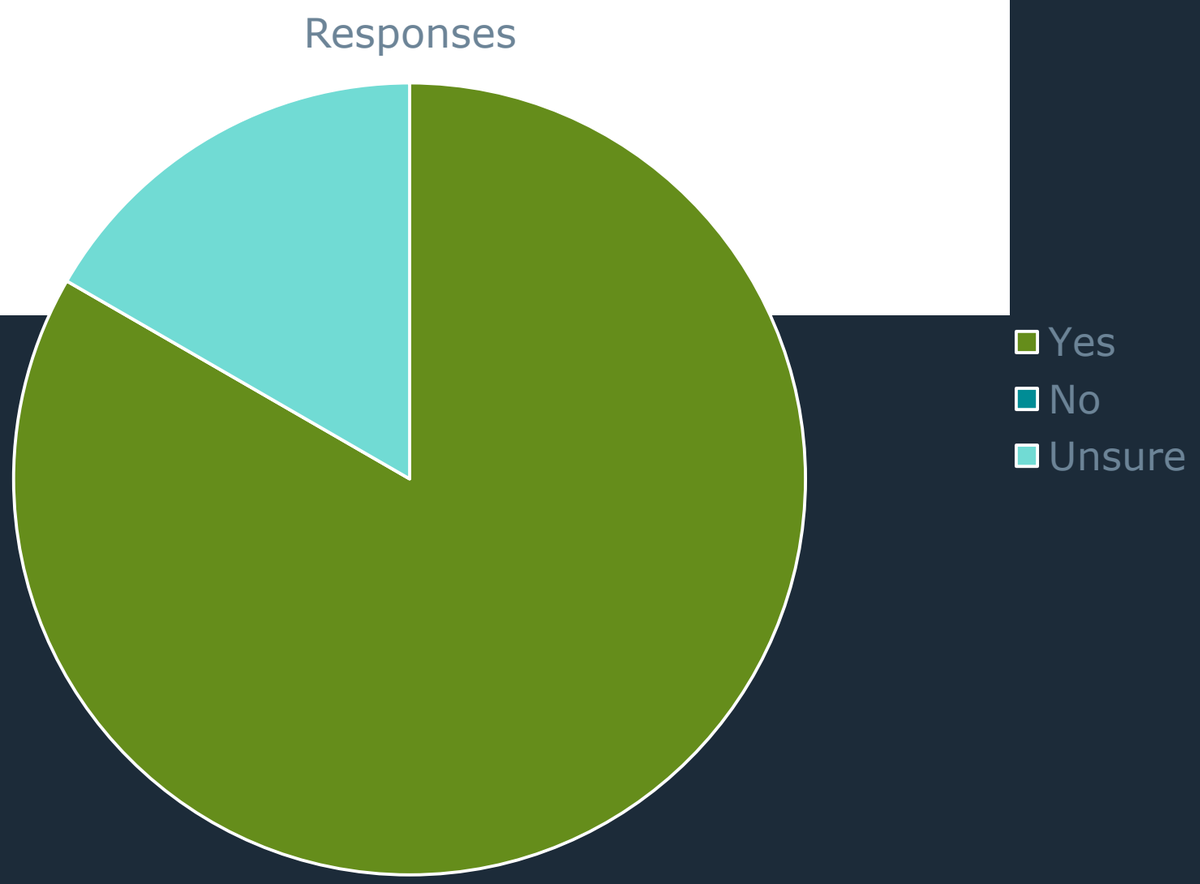
- Notification to a supervisory authority is mandatory "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons [data subjects]".
- Notification to data subjects is mandatory "when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons"

ashurst

Case studies – Scenario Two

2. **Scenario Two**: Following further investigations, you confirm that the client system has definitely been accessed and you also discover that the log in details to client portals for each of those clients have been accessed. Such details accessed include usernames, passwords and the client portal is used to issue TOB/policy documentation. Do you notify the ICO and/or data subjects?

- ◯ Yes
- ◯ No
- ◯ Unsure



Breach handling tips

Review your breach response procedure	Assemble your breach team	Other key tips
When was it last updated? Has it been updated since a previous breach?	Who makes up your breach team? I.e. who will be in the "war room" when a breach has been identified?	Assume the breach
Is there a clear step process?	Does it include at a minimum: DPO, Legal, CISO, ransomware negotiators, external legal counsel, PR for comms strategy and key decision makers – i.e. senior stakeholders who can decide to close/lock off systems.	Remember loss of availability = a breach
Have a template timeline built into your step by step process which require a "minute by minute" breakdown?	Are these people already identified and lined up?	Check your insurance policy to know what's covered – for example, are you required to use a certain law firm/forensic analyst? You don't want to fall foul and be uninsured.
Ensure it prompts you to record who discovered the breach	Are these people aware of their roles and responsibilities in the event of a breach?	Remember to adhere to local guidance
Ensure containment and mitigation are a key stage (system lockdown, preservation of documents, internal investigations, password changes, security of systems)	What are your procedures for when any of the relevant designated persons within your breach team are on holiday, out of the office or on sick leave?	Ring the ICO if you're not sure - discuss on a no named basis.
		To make a notification to the ICO, we recommend calling first on 0303 123 1113 and the ICO will follow up with a note of the conversation. The ICO hotline is open Monday – Friday between 9 am and 5 pm.
		As part of the breach, consider other implications: confidentiality, contractual obligations to third parties, FCA/other regulator notification? Spend time drafting the data subject notifications: avoid misleading language/usual reluctance of not providing information. This will be a preventative action to claims, data subject access requests and complaints.

Breach step by step process

First 24 hours

CONTAINMENT & RECOVERY

- Establish what has happened
- What can be done to limit the damage?
- Who will take the lead?

1

2

IDENTIFYING & ASSESSING THE RISKS

- Assess the likelihood of the risk
- Assess the severity of the risk

24 – 72 hours

72 hours onwards

INVESTIGATION & IMPLICATIONS

- Internal investigation
- Changes to security, policies and training
- Litigation
- PR strategy: for dealing with complaints

4

3

NOTIFICATIONS & COMMUNICATIONS

- ICO, FCA, other regulators.
- Affected persons
- Maintaining privilege
- Contractual requirements/suppliers
- Insurers
- Market announcement
- PR
- Employees

Ashurst Data Transfers Offering

1	2	3
Data mapping	**Defining data transfer strategy**	**Preparation of template key documents**
• Exercise to identify all data transfers: internal and external • Create your ‘data catalogue”	This involves: • determining whether clients treat UK and EU transfers separately or adopt a combined approach; • defining an organisation's risk profile and methodology; • determining approach for prioritisation in respect of (i) existing and new transfers; and (ii) type of transfer, based on risk framework; • determining approach for data transfer assessment; • determining approach for onwards transfers; and • implementing an approach for operationalisation and risk acceptance/sign off.	Key documents will include: • Transfer impact assessment/transfer risk assessments • Jurisdictional risk assessments • Playbook of data transfer contractual wording incorporating relevant data transfer mechanism • Menu of supplementary measures guidance.

Questions?

Rhiannon Webster
Partner and Head of Data Protection Practice

T +44 20 7859 3070
Rhiannon.Webster@ashurst.com

Jake Green
Practice Global Co-Head, Financial Regulatory

T +44 20 7859 1034
Jake.Green@ashurst.com

Shehana Cameron-Perera
Senior Associate, Digital Economy

T +44 20 7859 2768
Shehana.Cameron-Perera@ashurst.com

Please send questions direct to our speakers via the chat box