ashurst

Data Protection 2021 Roundup

24 NOVEMBER 2021

What today's session will cover

01. **INTERNATIONAL DATA TRANSFERS A YEAR IN REVIEW**

Kyra Bowman, Policy Advisor, DCMS

02. **2021 UK ICO GUIDANCE ROUNDUP**

Rhiannon Webster, Partner

03. **RETURN TO WORK, REMOTE WORKING & MONITORING EMPLOYEES**

Liz Parkin, Senior Associate

04. **KEY DATA BREACH CASES**

Sophie Law, Senior Associate

05. **UK ENFORCEMENT ACTIONS: LESSONS LEARNT**

Harry Newton, Associate

06. **SPOTLIGHT ON EUROPE: KEY GUIDANCE & ENFORCEMENT**

Andreas Mauroschat, Partner

ashurst

Department for
Digital, Culture,
Media & Sport

International Data Transfers

A Year in Review

Kyra Bowman, DCMS

UK Objectives

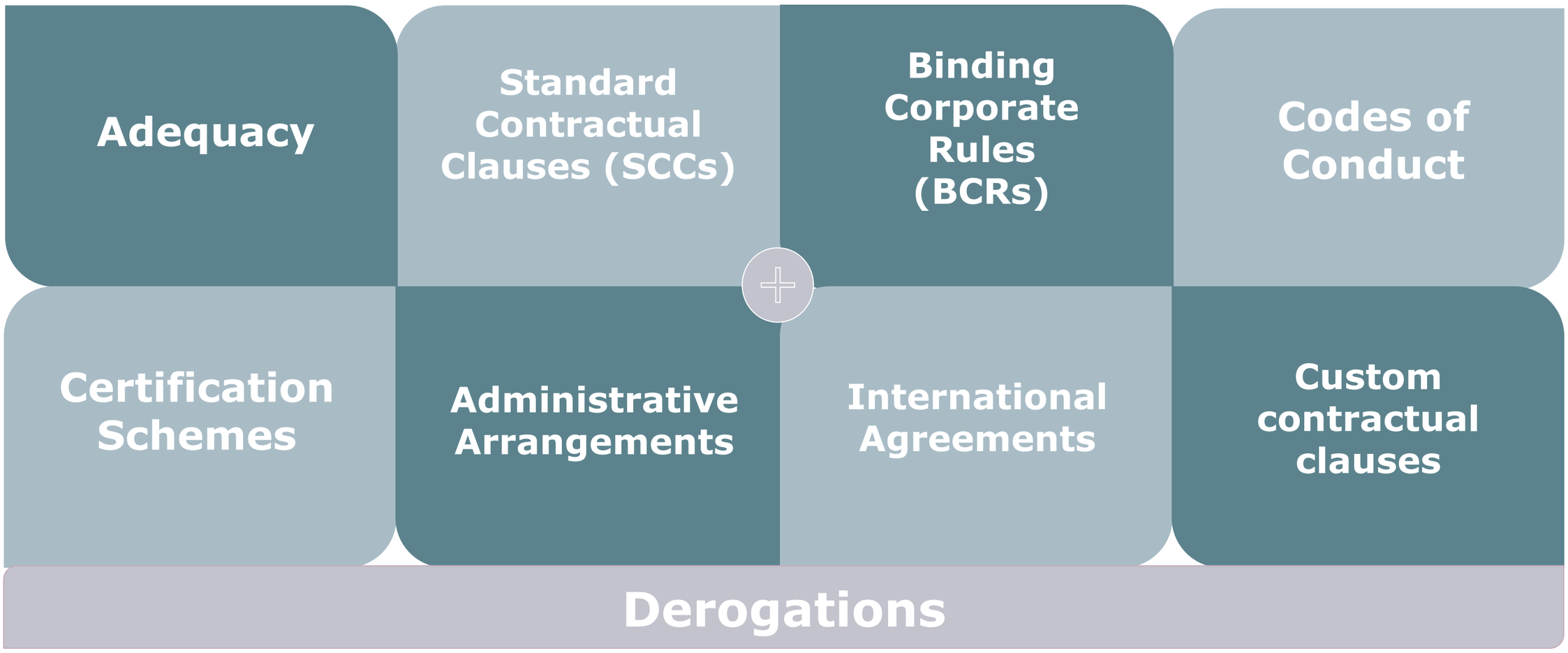
Build trust in the use of data

Facilitate cross-border data flows

Drive data standards and interoperability

Drive UK values internationally

The Current GDPR Toolbox



International Data Transfers in 2021

Secured EU Adequacy

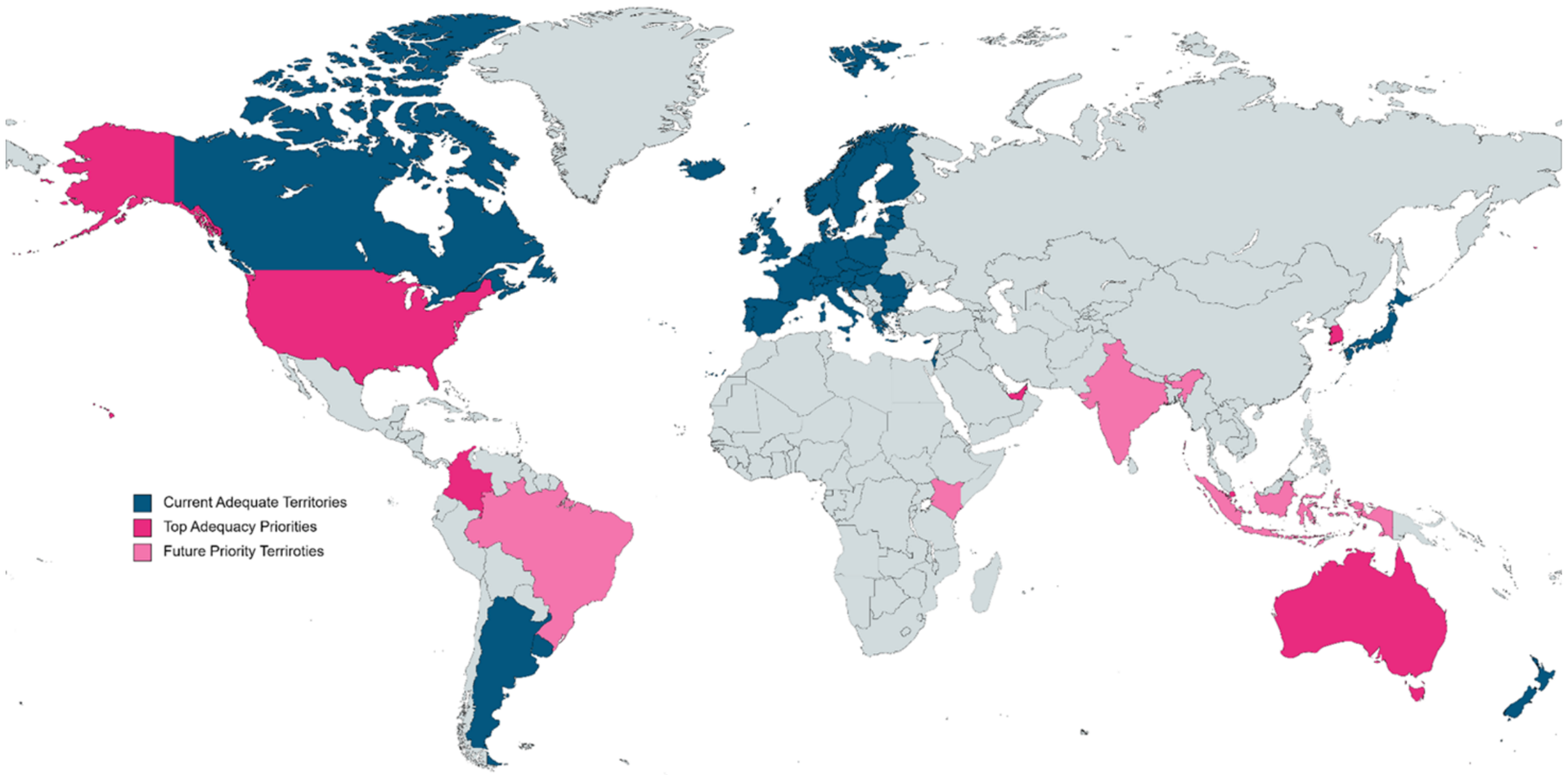
DCMS/ICO Memorandum of Understanding

Announcement of Adequacy Priority Countries

ICO Consultation on International Data Transfer Agreements

Announcement of IDT Expert Council

Adequacy Priority Countries



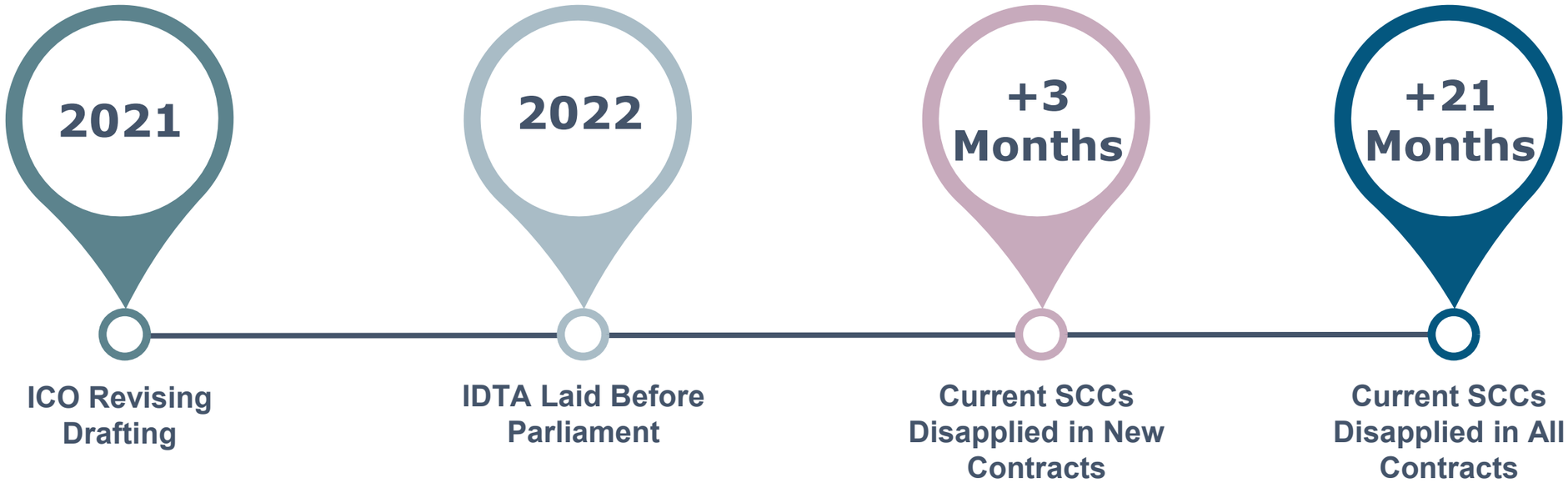
USA | **Colombia** | **DIFC** | **Singapore** | **Republic of Korea** | **Australia**

Brazil | **Kenya** | **India** | **Indonesia**

New UK International Data Transfer Agreements

1. User-friendly for non-expert users
2. Cover more transfer scenarios
3. Flexible and enables multi-party agreements
4. Pragmatic approach to Schrems II
5. Interoperable EU “bolt-on” clause

Implementing New UK IDTAs



International Data Transfers Expert Council

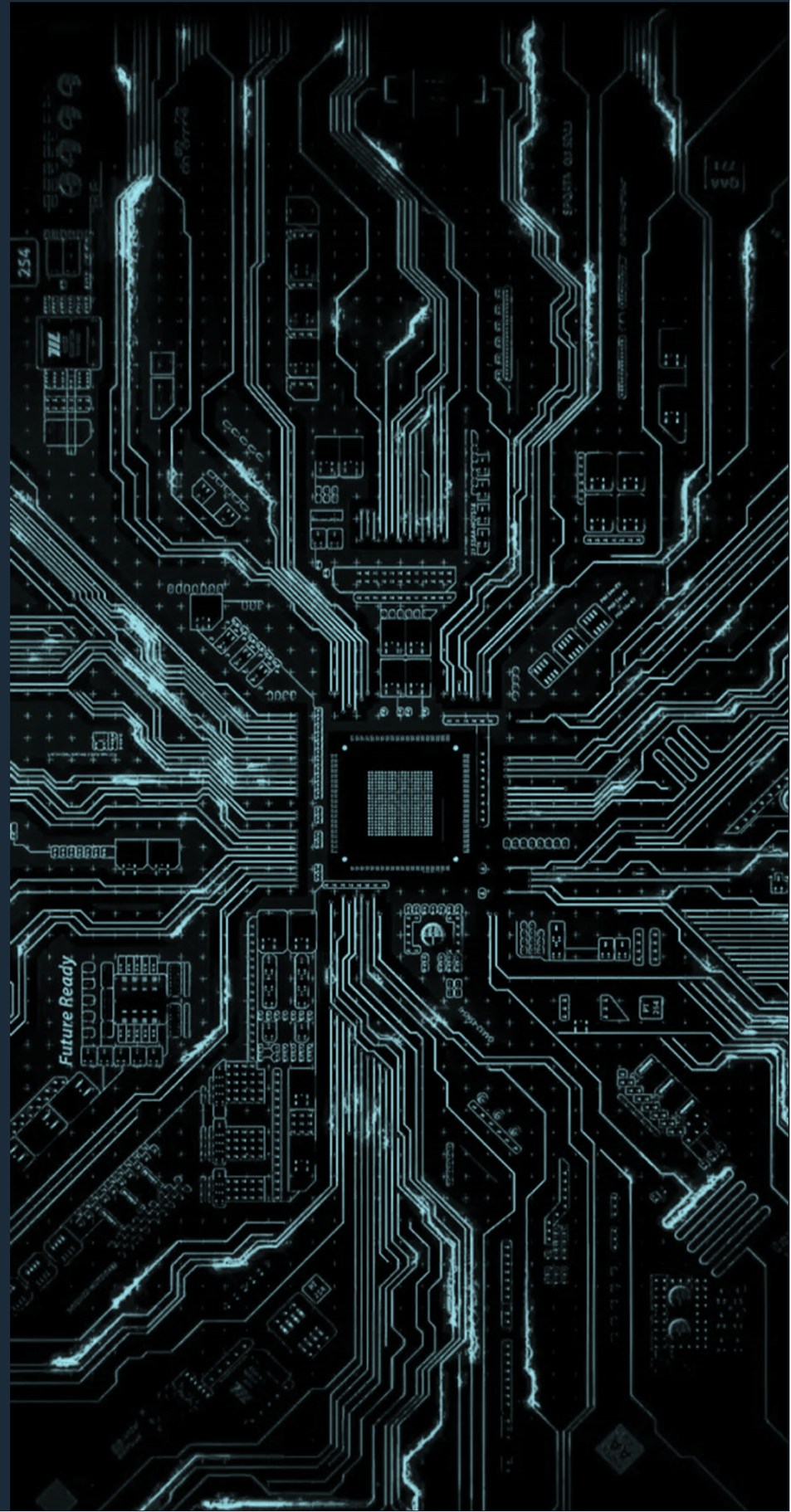
20 expert members drawn from **academia, industry and civil society**

Provide **independent and expert advice** to inform IDT policy

Department for
Digital, Culture,
Media & Sport

2021 UK ICO Guidance Roundup

Rhiannon Webster
Partner
Digital Economy Team



2021 Roundup: ICO Guidance and Codes

JAN 2021

11 MAR 2021

Release of the Use of Personal Data in Political Campaigning Guidance

28 MAY 2021

Consultation start date: Anonymisation, Pseudonymisation and Privacy Enhancing Technologies Guidance (*closing 28 Nov 2021*)

11 AUG 2021

Consultation start date: International Data Transfer Agreement and Guidance (*closed 11 Oct 2021*)

04 AUG 2021

Release of Direct Marketing and the Public Sector Guidance

05 OCT 2021

Data Sharing Code of Practice came into effect

SEP & OCT 2021

Release of the (1) Children's Code Best Interests Framework, (2) Design Guidance and (3) Opinion on How Age Assurance can Support Services to Conform to the Children's Code

13 OCT 2021

Consultation start date: Draft Journalism Code of Practice

DEC 2021

Source: ICO

2021 Roundup: Other ICO Releases

JAN 2021

17 FEB 2021
Release of the Data Analytics Toolkit

18 JUN 2021
ICO publishes opinion on the use of live facial recognition technology in public places

28 JUN 2021
ICO statement in response to the EU Commission's announcement on the approval of the UK's adequacy

20 JUL 2021
Release of AI Toolkit

15 JUL 2021
Release of Q&As – Vaccination and COVID Pass Checks

19 AUG 2021
Release of UK GDPR Certification Scheme Criteria

14 SEP 2021
Release of Sharing Personal Data in an Emergency – Guide for Universities and Colleges

27 OCT 2021
Release of Joint Statement on Global Privacy Expectations of Video Teleconferencing Companies

02 NOV 2021
Release of Framework for Analysing End to End Encryption in an Online Safety Context

DEC 2021

Source: ICO

Data Sharing Code of Practice

2011

ICO published its first data sharing code under the Data Protection Act 1998

23 MAY 2018

Publication of the Data Protection Act 2018, which included provisions requiring the ICO to produce a data sharing code of practice

JUL 2019

First draft of the new Code went out to consultation

17 SEP 2020

ICO submitted the Data Sharing Code of Practice to the Secretary of State

05 OCT 2021

Data Sharing Code of Practice came into effect

Key information:

- ✓ Statutory code of practice under section 121 of the Data Protection Act 2018.
- ✓ The ICO must therefore take the Code into account when considering whether there has been compliance with data protection obligations when sharing data. A Court must also take the Code into account where relevant, and it can be used in evidence in court proceedings.

Source: ICO

Data Sharing Code of Practice

KEY CONCEPTS IN THE CODE

1. **Scope: Sharing between controllers,** not between a controller and processor. Covers routine/systemic, one off and data pooling.
2. Recommendation that **data protection impact assessments** are undertaken
3. **Good practice but not mandatory to have a data sharing agreement in place**. The ICO will consider whether there is a data sharing agreement in place when assessing any data sharing arrangements, for example, following a complaint.
4. **Effective accountability**
5. **Individuals' rights:** The data sharing arrangements must encompass policies and procedures that allow data subjects to exercise their individual rights easily, and this must be communicated to them (for example, privacy notices should make clear which organisation to contact; the Code suggests a single point of contact is good practice).
6. **Mergers and Acquisitions:** The Code provides some brief guidance on data sharing arising from a merger or acquisition or other change in organisational structure, when data may need to be transferred to a different organisation. The data sharing must be considered as part of the due diligence, and the Code provides a checklist of issues to consider.
7. **Sharing personal data in databases and lists:** When receiving personal data in databases and lists, the recipient organisation is responsible for complying with data laws and must therefore satisfy itself as to the integrity of the data.
8. **Children's data:** Extra care must be taken when sharing children's data – controllers must be able to demonstrate a compelling reason to do so, taking account of the best interests of the child. Again, a DPIA will ensure proper risk assessment and mitigation.

Source: ICO

Anonymisation, pseudonymisation & privacy enhancing technologies guidance

CONSULTATION START DATE: 28 MAY 2021 | CONSULTATION CLOSE DATE: 28 NOVEMBER 2021

- ✓ The guidance is intended to help organisations identify the issues they need to consider to use anonymisation techniques effectively, and will sit alongside the ICO's data sharing code of practice.
- ✓ The ICO has so far published two draft chapters, as follows:

CHAPTER ONE

Introduces and defines anonymisation and pseudonymisation, and places the concepts within the framework of data protection law in the UK.

CHAPTER TWO

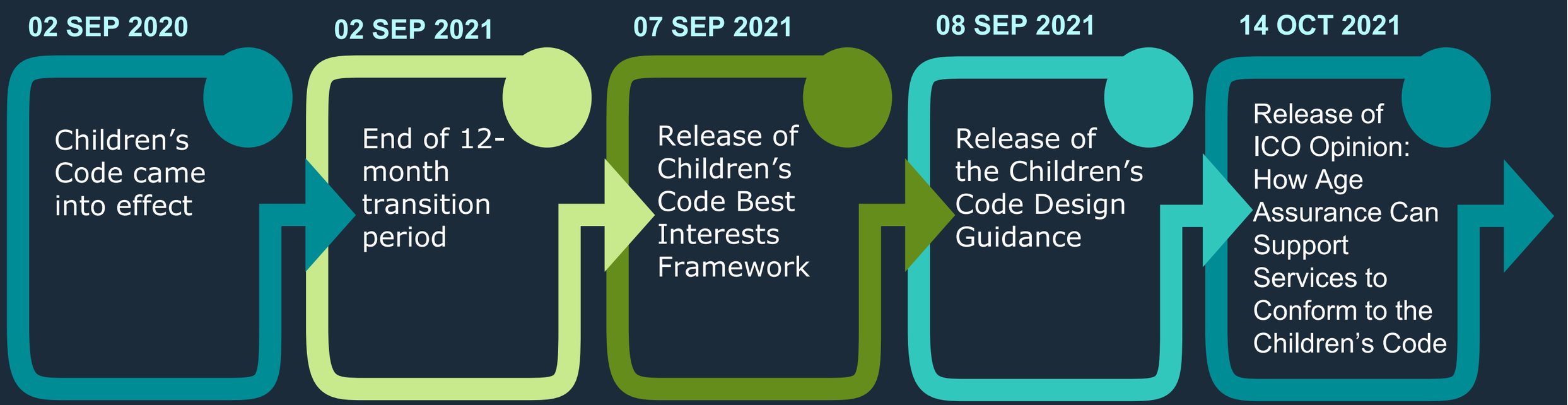
Focuses on how to assess anonymisation in the context of identifiability.

Source: ICO

The Children’s Code (Age Appropriate Design Code)

Key information:

- ✓ Data protection code of practice for online services (including apps, games, social media platforms, streaming and news services) likely to be accessed by children
- ✓ Needs to be considered if children are likely to access a particular service, even if that service is not targeted at children
- ✓ Applies to UK-based companies and non-UK based companies who process the personal data of UK children



Source: ICO

ashurst

The Children’s Code (Age Appropriate Design Code)

FLEXIBLE STANDARDS

1. **The best interests of the child** should be the primary consideration
2. **Data protection impact assessments must be embedded**
3. **Age appropriate application**
4. **Transparency**
5. **No detrimental use of data**
6. Uphold **policies and community standards**
7. Settings must be **‘high privacy’ by default**
8. **Data minimisation**
9. **Data sharing** avoided
10. **Geolocation** options should be turned off by default. Children should be able to see when location tracking is active
11. Where **parental controls** are provided, organisations must give the child age appropriate information about this. If parents or carers can monitor a child’s online activity the child should be able to see when they are being monitored
12. Options which use **profiling** should be switched ‘off’ by default
13. Avoid **nudge** techniques
14. **Connected toys and devices** also in scope
15. **Online tools** for children to exercise their rights and concerns

Source: ICO

International Data Transfer Agreements

A SUMMARY OF THE YEAR

- ✓ UK were granted adequacy therefore transfers of personal data from the EU to UK can continue without further steps

- ✓ EU Commission have published new model clauses which must be used for all new transfers from Europe to non adequate countries

- ✓ Data exporters and data importers in Europe have **until 27 December 2022** to replace contracts using the current standard contractual clauses with the new clauses - unless the actual underlying processing operations change, in which case the clauses should be used from that point on

- ✓ The UK have published a UK data transfer agreement for the same purpose (and an alternative addendum to the EU model clauses). Consultation has closed. **Awaiting final form**

- ✓ Current status is that for transfers from the UK to be compliant, the correct model clauses are the **Old EU model clauses**

- ✓ **Transfer Impact Assessments** should be undertaken for all transfers occurring under model clauses and binding corporate rules (NB: both UK and EU)

Source: ICO

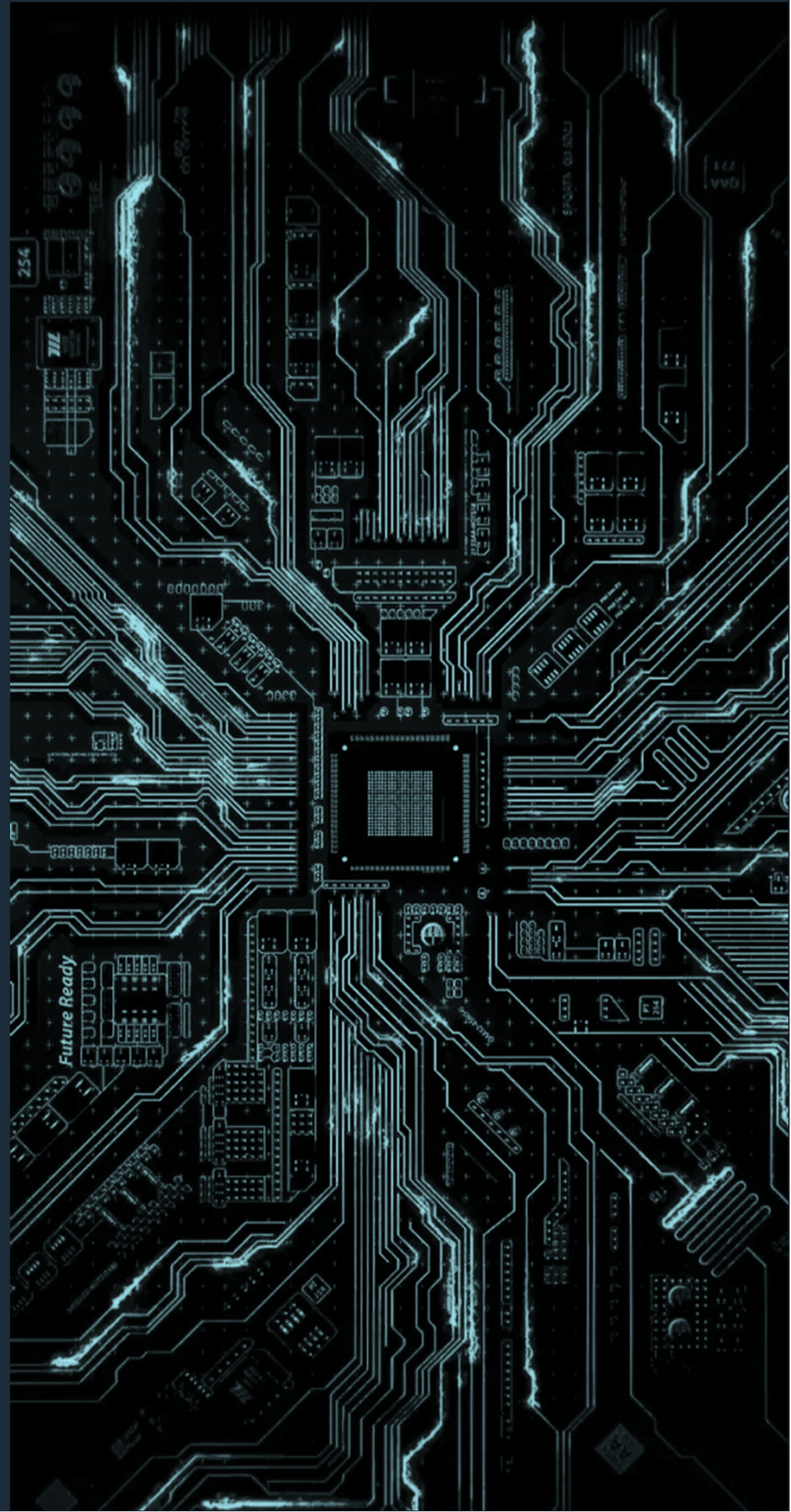
What’s next for 2022

- A new Information Commissioner: John Edwards (former privacy commissioner of New Zealand)
- A more settled position on international transfers from the UK
- New regulatory action policy currently being drafted (2021-2024)
- Data: a new direction: The government has launched a consultation on reforms to create an ambitious, pro-growth and innovation-friendly data protection regime that underpins the trustworthy use of data.

Source: ICO

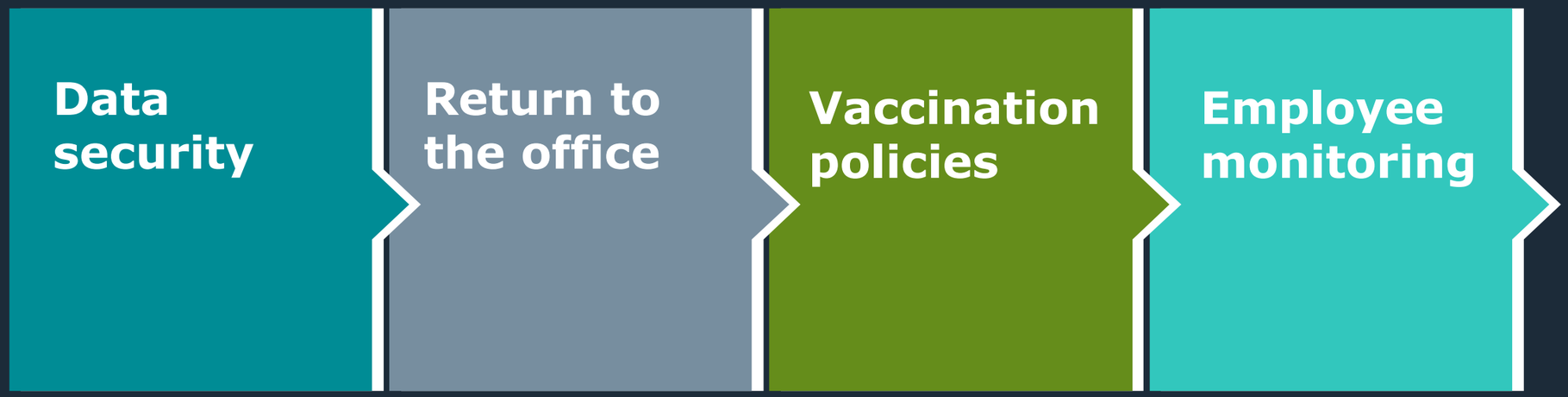
Returning to work, remote working and monitoring employees

Liz Parkin
Senior Associate
Employment



Key employment impacts of Covid-19

ISSUES FOR EMPLOYERS



ashurst

Return to the office

EMPLOYER REQUIREMENTS

ashurst

Covid status questions

WHAT CAN WE ASK

ashurst

Vaccinations and the workforce

KEY QUESTIONS FOR EMPLOYERS

1. What is meant by requiring employees to be vaccinated?
2. Is a compulsory vaccination policy appropriate?
3. Would there need to be exemptions from compulsory vaccinations?
4. How would compulsory vaccination be implemented?
5. Can employers permit only vaccinated employees to return to the workplace?
6. Can employers insist that employees who are not vaccinated continue to work remotely?
7. Where only vaccinated employees return to the workplace, do all employees have a right to be paid?
8. Can employers ask for proof of vaccination?
9. Can employers record who has been vaccinated and who has not?
10. Are employers able to adopt a different position with contractors and consultants?

ashurst

Monitoring remote working

MONITORING METHODS

- Checking how long employees are logged in for
- Recording calls
- Checking what websites are visited
- Logging keystrokes
- Requiring time-recording on a self-reporting basis
- Taking regular screenshots
- Recording which electronic files are accessed
- GPS tracking
- Checking emails e.g. how many are sent, to whom and when and/or looking for specific words in emails
- Webcam surveillance

General Data Protection Regulation (GDPR)

THE RELEVANT PRINCIPLES

1 **Data must be processed lawfully, fairly and in a transparent manner**

2 **Collected only for specified, explicit and legitimate purposes**

3 **Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.**

4 **Processed in a manner that ensures appropriate security**

ashurst

Carrying out a Data Protection impact assessment

A data protection impact assessment is required under the GDPR where the processing is likely to result in a high risk to the individual's rights and freedoms.

Issues to address in the impact assessment:

1

What?

What monitoring will be carried out?

2

Why?

Identify the purpose(s) for the monitoring

3

Is monitoring necessary?

Could the purpose you have identified be achieved without monitoring?

4

Less intrusive alternatives?

Is there a way of monitoring that achieves the identified purpose but is less intrusive?

5

Impact on employees

Consider what impact the monitoring might have on employees

6

Is it justified?

Do the benefits for the employer outweigh the adverse impact on employees?

Additional GDPR points

Provide employees with **clear and full information**

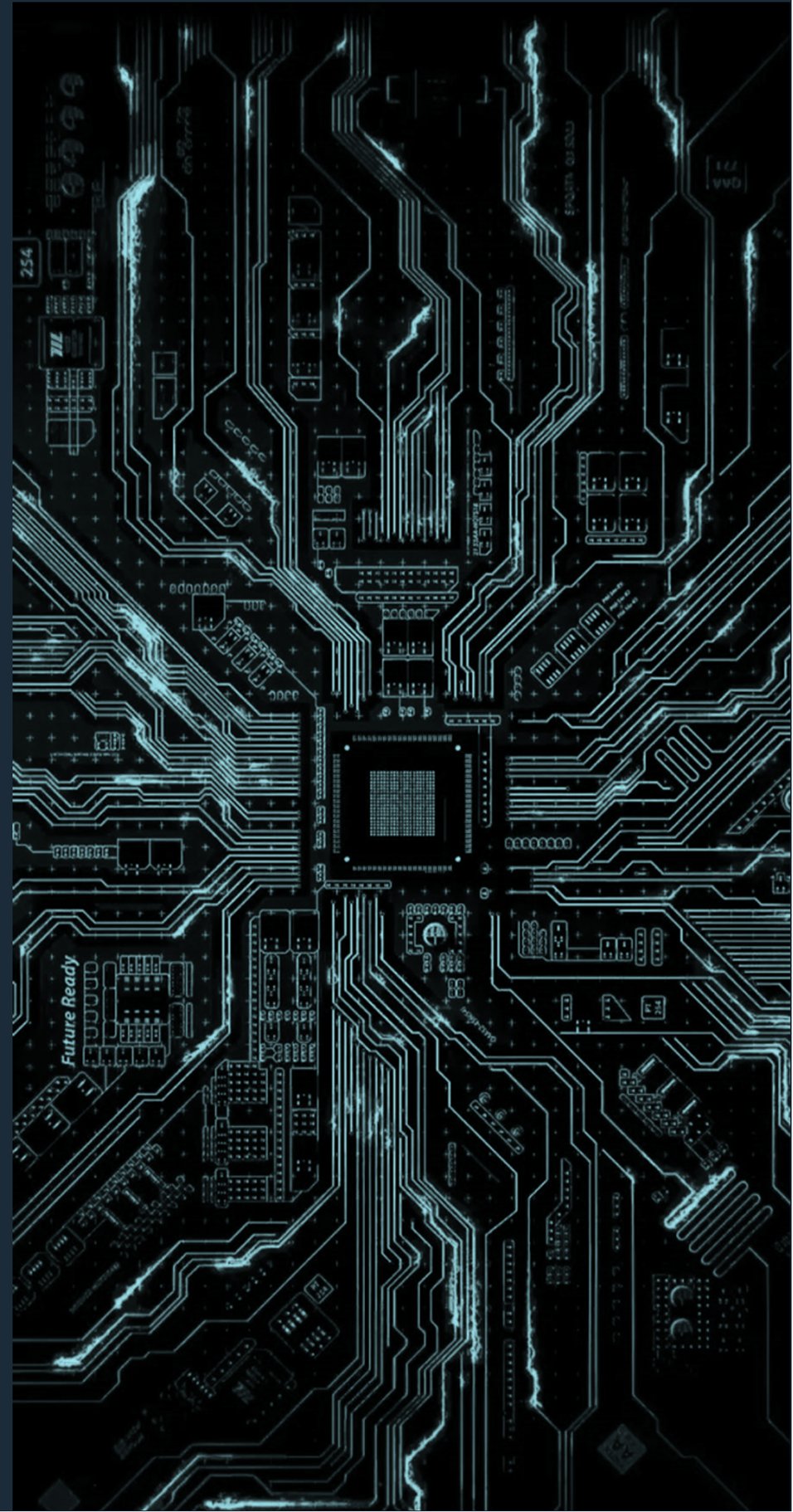
Keep the information **secure**

Do not use information **acquired for one purpose** for another purpose

Remember: the financial penalties for breaching the GDPR can be very substantial

Key data breach cases

Sophie Law
Senior Associate
Disputes



KEY CASES

1. **Warren v DSG Retail Ltd** [2021] EWHC 2168

2. **Rolfe & Ors v Veale Wasbrough Vizards LLP** [2021] EWHC 2809 (QB)

3. **Lloyd v Google LLC** [2021] UKSC 50

Warren v DSG Retail Ltd [2021] EWHC 2168

A NARROWING OF THE SCOPE OF DATA BREACH CLAIMS ARISING FROM HACKING CASES?

Breach of Confidence / Misuse of Private Information

- Cannot succeed without "use" or "misuse" of the information by the Defendant
- Failure to secure data (i.e. an omission or a failure to act) is not "use"
- No data security duty

Negligence

- No need to impose a duty of care where there were already statutory duties in place
- No claim for personal injury

Data Protection Act 1998

- Permitted to proceed

Potential impact on litigation funding / ATE?

ashurst

Rolfe & Ors v Veale Wasbrough Vizards LLP [2021] EWHC 2809 (QB)

THE LAW WILL NOT SUPPLY A REMEDY WHEN NO HARM HAS CREDIBLY BEEN SHOWN

*"What harm has been done, arguably? We have here a case of **minimally significant information**, nothing especially personal such as bank details or medical matters, **a very rapid set of steps to ask the incorrect recipient to delete it** (which she confirmed) and **no evidence of further transmission or any consequent misuse** (and it would be hard to imagine what significant misuse could result, given the minimally private nature of the data). We have **a plainly exaggerated claim** for time spent by the Claimants dealing with the case and a **frankly inherently implausible suggestion that the minimal breach caused significant distress** and worry or even made them 'feel ill'. … There is **no credible case that distress or damage over a de minimis threshold will be proved**. In the modern world it is not appropriate for a party to claim, (especially in the High Court) for breaches of this sort which are, frankly, **trivial**. The case law referred to above provides ample authority that whatever cause of action is relied on **the law will not supply a remedy in cases where effectively no harm has credibly been shown or be likely to be shown**."*

Lloyd v Google LLC [2021] UKSC 50

NO DAMAGES SIMPLY FOR LOSS OF CONTROL

'Loss of Control' damages

- Cannot claim compensation merely for contravention of DPA 1998
- Must prove that the contravention has caused material damage or distress

Representative action: same interest?

- Declaration of liability possible but not damages
- Damage requires individual assessment
- Alternative approach to representative actions

"… the claimant seeks damages under section 13 of the DPA 1998 for each individual member of the represented class ***without attempting to show that any wrongful use*** *was made by Google of personal data relating to that individual or* ***that the individual suffered any material damage or distress*** *as a result of a breach of the requirements of the Act by Google. For the reasons explained in this judgment, without proof of these matters,* ***a claim for damages cannot succeed****."*

ashurst

What next for data breach claims?

1 **Does Lloyd v Google apply under GDPR?**

2 **General trend – tsunami to trickle?**

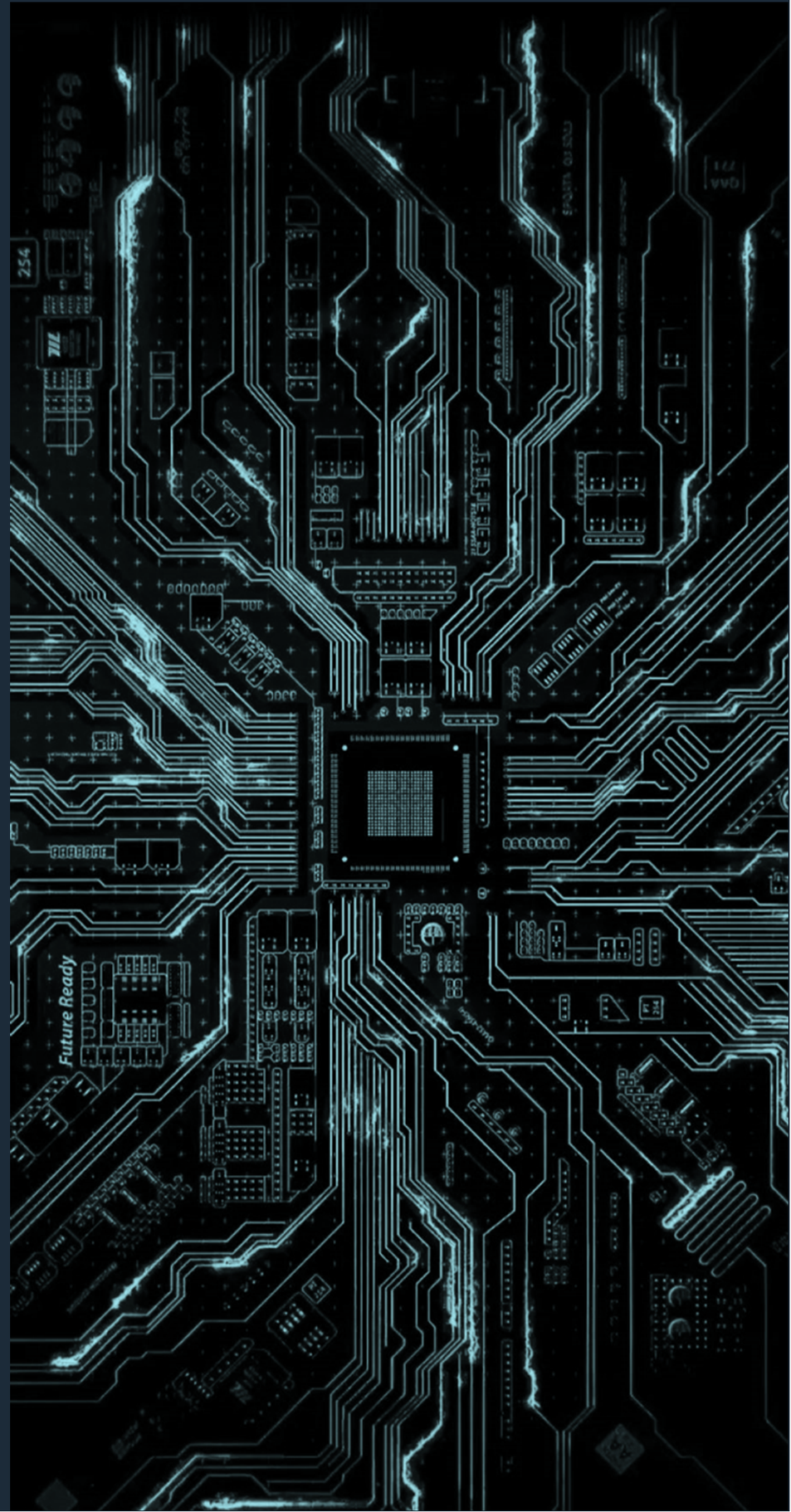
3 **How will group data claims now be framed? Litigation funding impact?**

4 **Procedural gap – call for legislative reform?**

ashurst

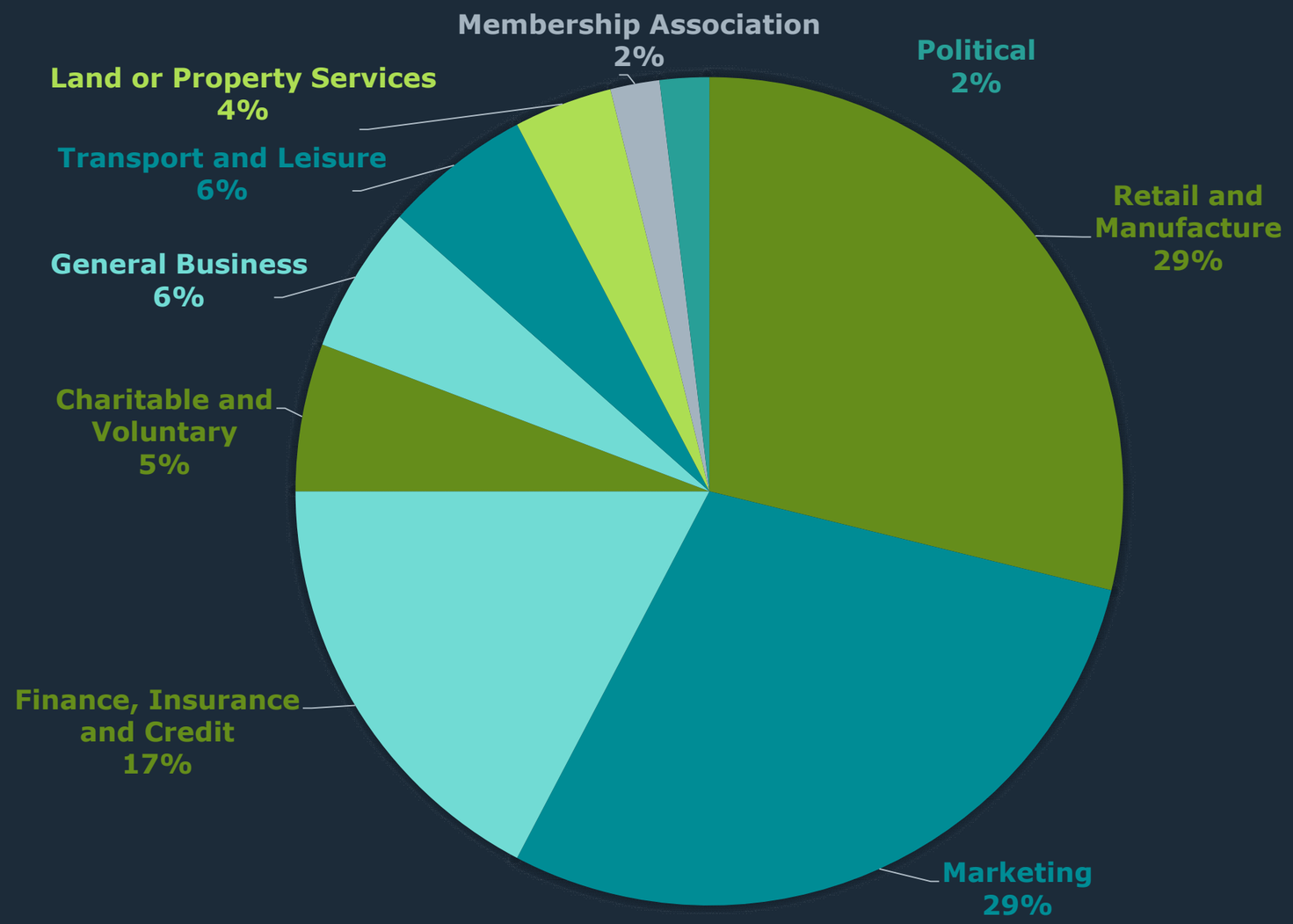
Lessons to be learnt from enforcement actions in the UK

Harry Newton
Associate
Digital Economy Transactions



Enforcement Industries

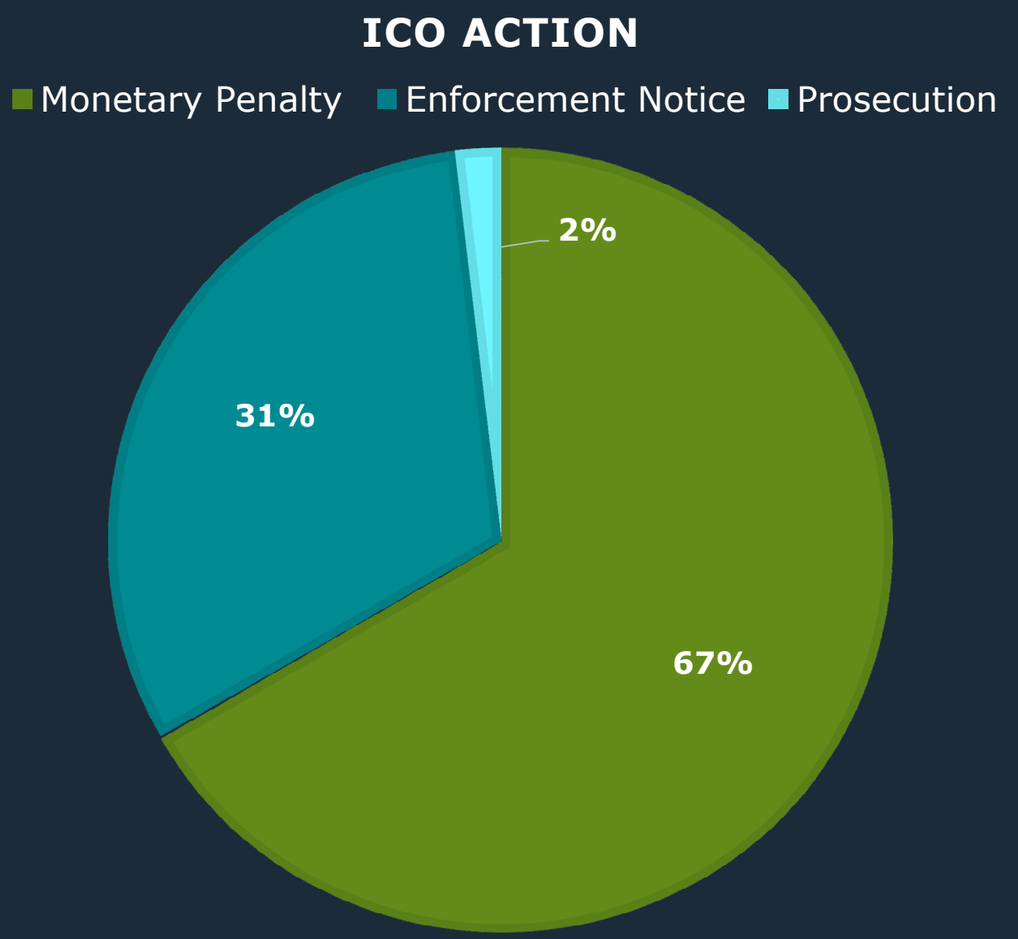
BASED ON NUMBER OF ACTIONS IN EACH INDUSTRY (NOV 2020 – NOV 2021)



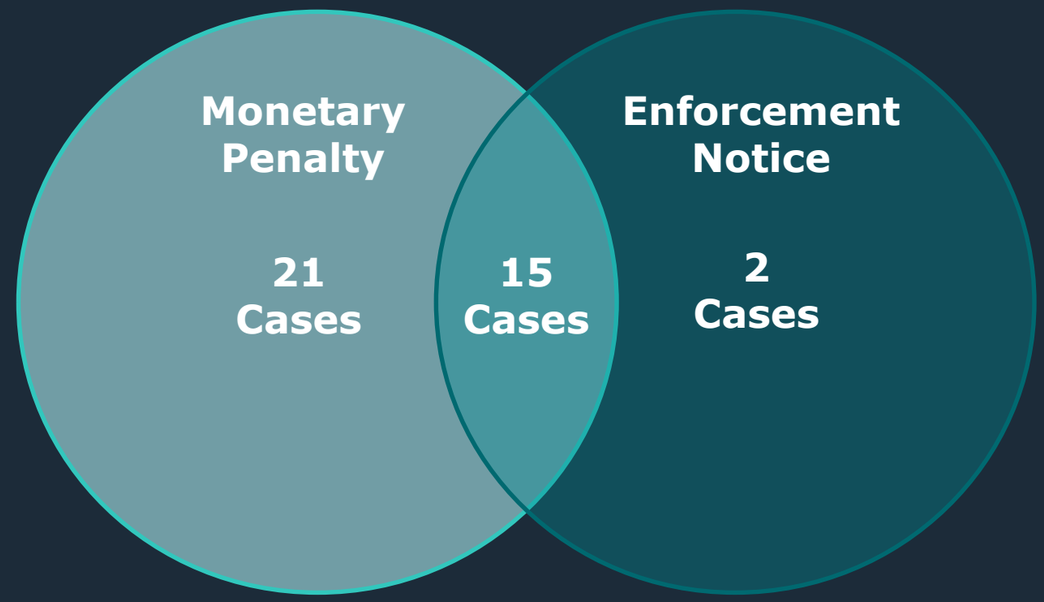
ashurst

ICO Action

NOV 2020 – NOV 2021



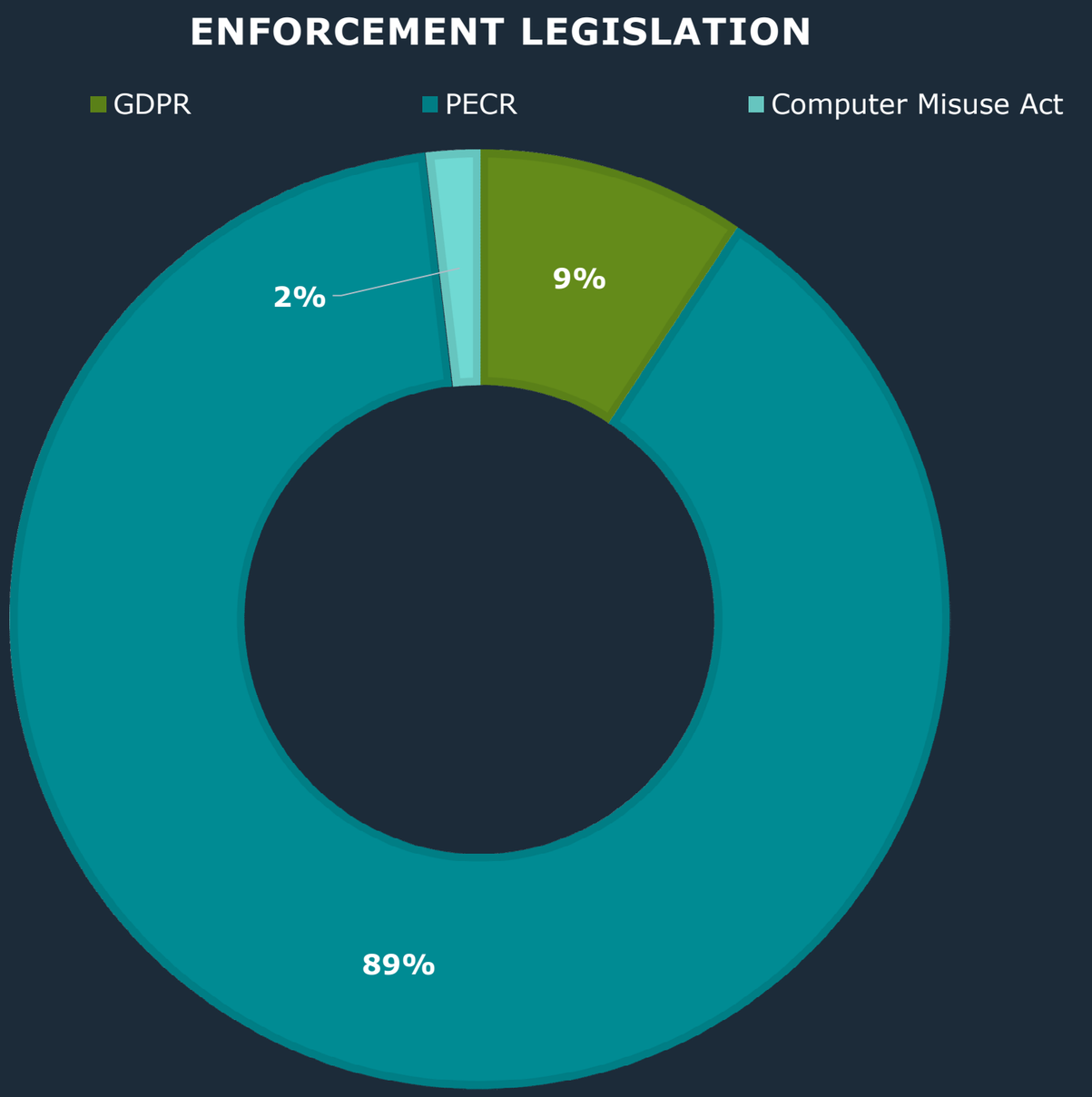
Overlap between monetary penalties and enforcement notices issued



ashurst

Enforcement Trends

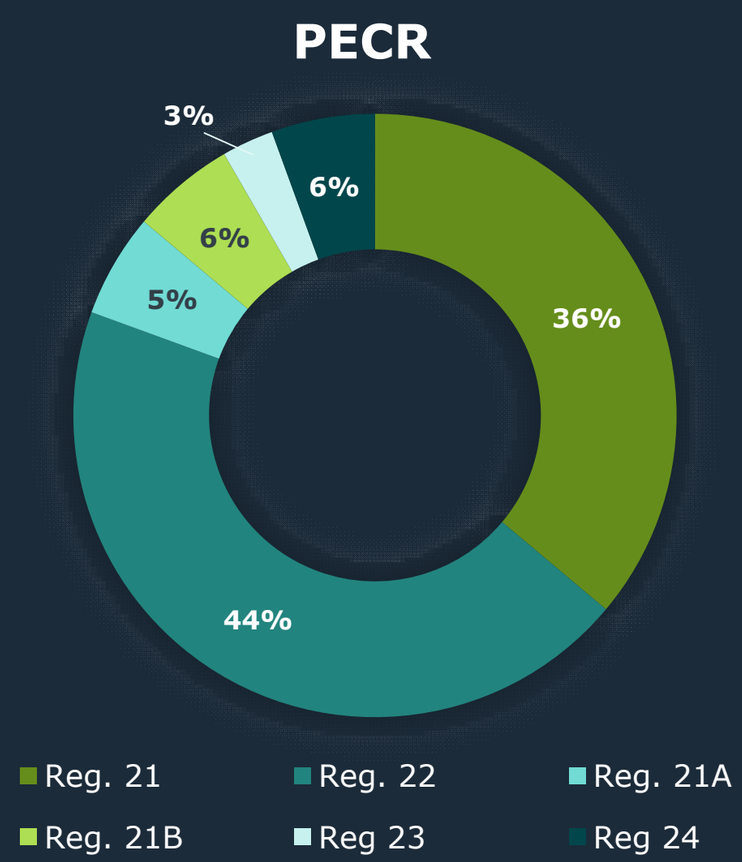
TREND OF ENFORCEMENT UNDER PECR VERSUS UK GDPR



ashurst

Enforcement Trends - PECR

NOV 2020 – NOV 2021

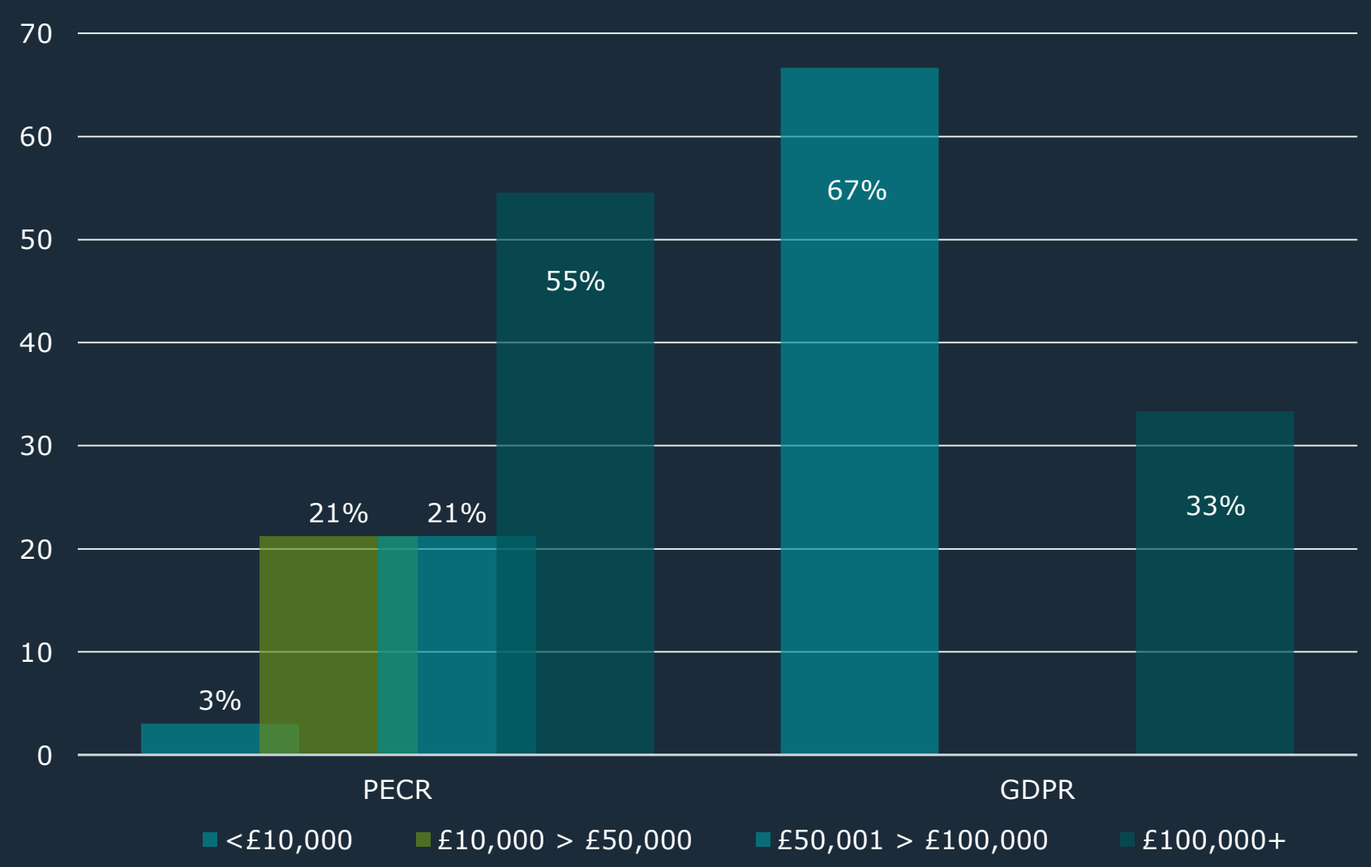


Regulation	Summary
Reg. 21	**Unsolicited phone calls for direct marketing**
Reg. 22	**Unsolicited electronic mail communications**
Reg. 21A	Unsolicited phone calls for direct marketing in relation to claims management services
Reg. 21B	Unsolicited phone calls for direct marketing in relation to pension schemes
Reg. 23	Use of email for marketing where the identity of the sender is concealed
Reg. 24	Concerns the information to be provided when making marketing calls under Reg. 21

Monetary Penalties

NOV 2020 – NOV 2021

- Under PECR, the ICO can enforce a fine of up to £500,000.
- Under the UK GDPR, fines can be issued of up to £17.5 million or 4% of the global turnover of the company.



ashurst

Enforcement under the UK GDPR

MONETARY PENALTY VERSUS ENFORCEMENT NOTICE

Monetary Penalty	Enforcement Notice

• Contraventions of Article 32 (data and security breaches) appear to warrant a monetary penalty.
 	
• Ticketmaster UK Limited, Mermaids and HIV Scotland were all issued with penalties as an "effective, proportionate and dissuasive" measure to deter against future breaches.
 	
• Amount of fines
  • Ticketmaster - £1.25 million
  • Mermaids - £25,000
  • HIV Scotland - £10,000
	• The trend shows that ICO has favoured enforcement notices for contraventions of certain other data processing requirements and principles under the UK GDPR.
	
	• Emailmovers Limited – Contravention of Article 5 requiring personal data to be processed "lawfully, fairly and in a transparent manner in relation to the data subject."
	
	• First Choice Selection Services Ltd – Contravention of Article 15 (failing to comply with a subject access request in breach of Article 15).

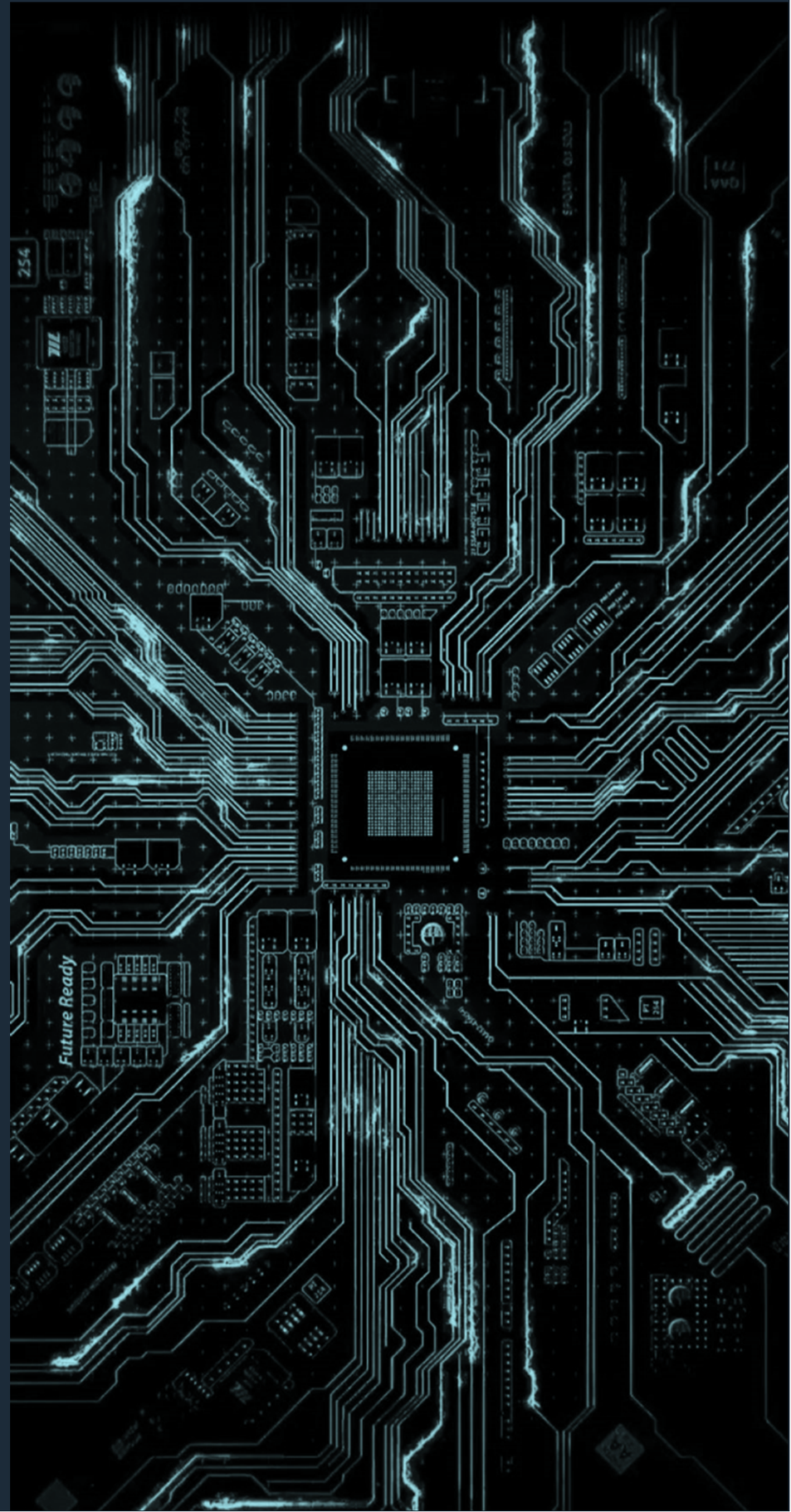
Enforcement under PECR

Aggravating Factors	Mitigating Factors
Lack of Cooperation and Openness with ICO • Lack of appropriate engagement with Commissioner during the course of an investigation	**Immediate Cooperation and Cessation of Breach** • Remedial action taken as soon as the contravention was highlighted
Ignorance of Publicly Available Advice • Taking into consideration guidance which is freely available on the ICO website	**The Degree to which the Breach was Institutional** • Whether the breach was the result of one or a few members of the organisation, or due to organisational policy
Previous Breaches • Taking into consideration previous breaches of the same regulations, which means that the company should have been "especially aware" of the regulation	**Due Diligence of Data Collected** • Evidence that the company carried out due diligence on third party data suppliers/third party data

Spotlight on Europe

Key guidance & enforcement

Andreas Mauroschat
Partner
Frankfurt/EU



2021 Enforcement Overview

- **Highest fine** in GDPR history for Amazon by Luxembourg DPA (EUR 746 million)
- **Number of fines** will likely top 2020: 360 until today
- Very few fines in connection with data transfers and scope of GDPR
- **High risk areas**:
  - insufficient legal basis
  - insufficient data security standards
  - insufficient fulfilment of data subject rights

2021 Enforcement - Direct Marketing

MAJOR PENALTIES

Sky Italia	Caixabank Spain	Unser Ö-Bonus Club
• EUR 3.2 mn monetary penalty • Sky Italia cold-called individuals using contact details from a purchased address list without quality checking the list • Seller had claimed individuals had consented. In fact, many of the listed individuals had expressly objected to being contacted	• EUR 3 mn monetary penalty • Caixabank created profiles of individuals to create targeted direct marketing content • Individuals had consented to the use of their data for direct marketing, but Caixabank had not explained that data from other sources would be used to create a profile	• EUR 2 mn monetary penalty • Club used customer loyalty scheme to create profiles for purposes of direct marketing • Information on profiling was given below the consent declaration on website which created the impression consent was given to receive special offers
Italian DPA held that: • Sky Italia had failed to notify individuals about the source of information and to obtain their consent • Sky Italia had also failed to check their own blacklist	Spanish DPA held that: • Individuals had not been fully and transparently informed and consent was not effective	Austrian DPA held that: • Consent declaration was not in plain and easy language and misleading

2021 – Court practice on DSAR

SCOPE HAS BEEN WIDENED – STILL MUCH UNCERTAINTY

BGH widened DSAR scope:	Personal data must be interpreted widely and also cover subjective information, internal notes and memos. Copies of legal advice/internal legal discussion excluded. Claim against insurance.
BAG:	Employee claimed copy of all emails containing his PD. Court left open if right to receive a copy, but held that claim for copies of "all emails" is not specific enough.
OLG Munich:	DSAR covers telephone notes, file notes, meeting protocols, emails, letters and subscription documents. Claim against investment firm.
LG Bonn:	Delayed response to DSAR as such is not a basis for immaterial damage claims. Claimant must provide facts to prove specific impairment.
Abusive DSARs:	No consistent court practice yet. Some courts consider DSAR abusive, if other targets are pursued than exercise of data subject rights.

2021 - EDPB Guidance

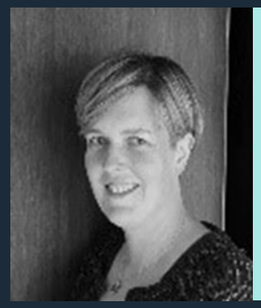
MOST RELEVANT GUIDANCE FOR COMPANIES

Consultation on Guidelines 05/2021: Interplay between Article 3 and international transfers	• Criteria and practical examples to identify data transfers • If transfer: requirements apply, regardless of whether importer is subject to the GDPR under Article 3 • But: transfer safeguards do not need to "duplicate" GDPR
08/2020: Targeting of social media users	• Targeting rules for social media providers and users, targeters and other actors such as adtech companies
01/2020: Connected vehicles and mobility apps	• Rules for processing of data inside vehicle, exchange between vehicle and personal devices and export of vehicle data

2021 - EDPB Guidance

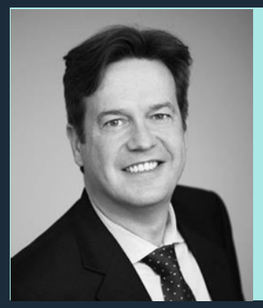
07/2020: Concepts of Controller and Processor	• Guidance and practical examples (e.g. law firms, cloud providers, headhunters)
01/2021: Data Breach Notification Examples	• Provide 18 illustrative case studies • Recommend measures to prevent/mitigate breaches
Recommendations 01/2020 – Supplementary Safeguards and Recommendations 02/2020 – European Essential Guarantees	• "Fallout" from Schrems II decision • Implemented in new Standard Contractual Clauses

Questions



Rhiannon Webster
Partner, London

T +44 20 7859 3070
M +44 7917 005 541
rhiannon.webster@ashurst.com

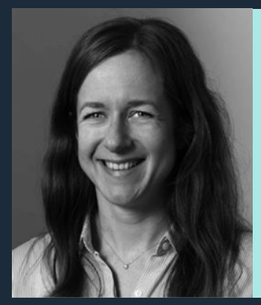


Andreas Mauroschat
Partner, Germany

T +49 69 97 11 28 19
M +49 172 43 54 666
andreas.mauroschat@ashurst.com

Liz Parkin
Senior Associate

T +44 20 7859 3413
M +44 7831 420 353
liz.parkin@ashurst.com



Sophie Law
Senior Associate

T +44 20 7859 2549
M +44 7771 905 834
sophie.law@ashurst.com

Harry Newton
Associate

T +44 20 7859 2703
M +44 7823 341 170
harry.newton@ashurst.com

ashurst

ashurst