

# GDPR – 4 Years On

*A CalQRisk Webinar*



Presented by:

Fiona Kiely, Senior Research Analyst, CalQRisk

Gerard Joyce, Chief Technical Officer, CalQRisk

# Webinar Agenda

Who we are

Overview 2018 – 2022

Changes in the Geopolitical Landscape

Technical & Organisational Measures

What's Next?

Q&A

# Who We Are

Experienced Risk & Compliance Professionals

Members of IRM, IoB, PRMIA, Compliance IRL, IOD, ACCA, ISACA..

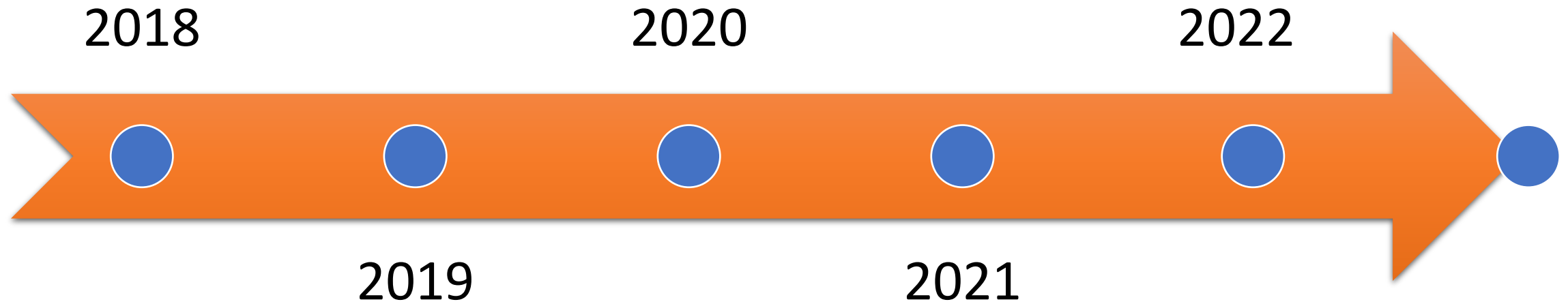
Involved in the Development of Standards (ISO 31000)

Supply a Governance, Risk & Compliance Software Solution  
called **CalQRisk**

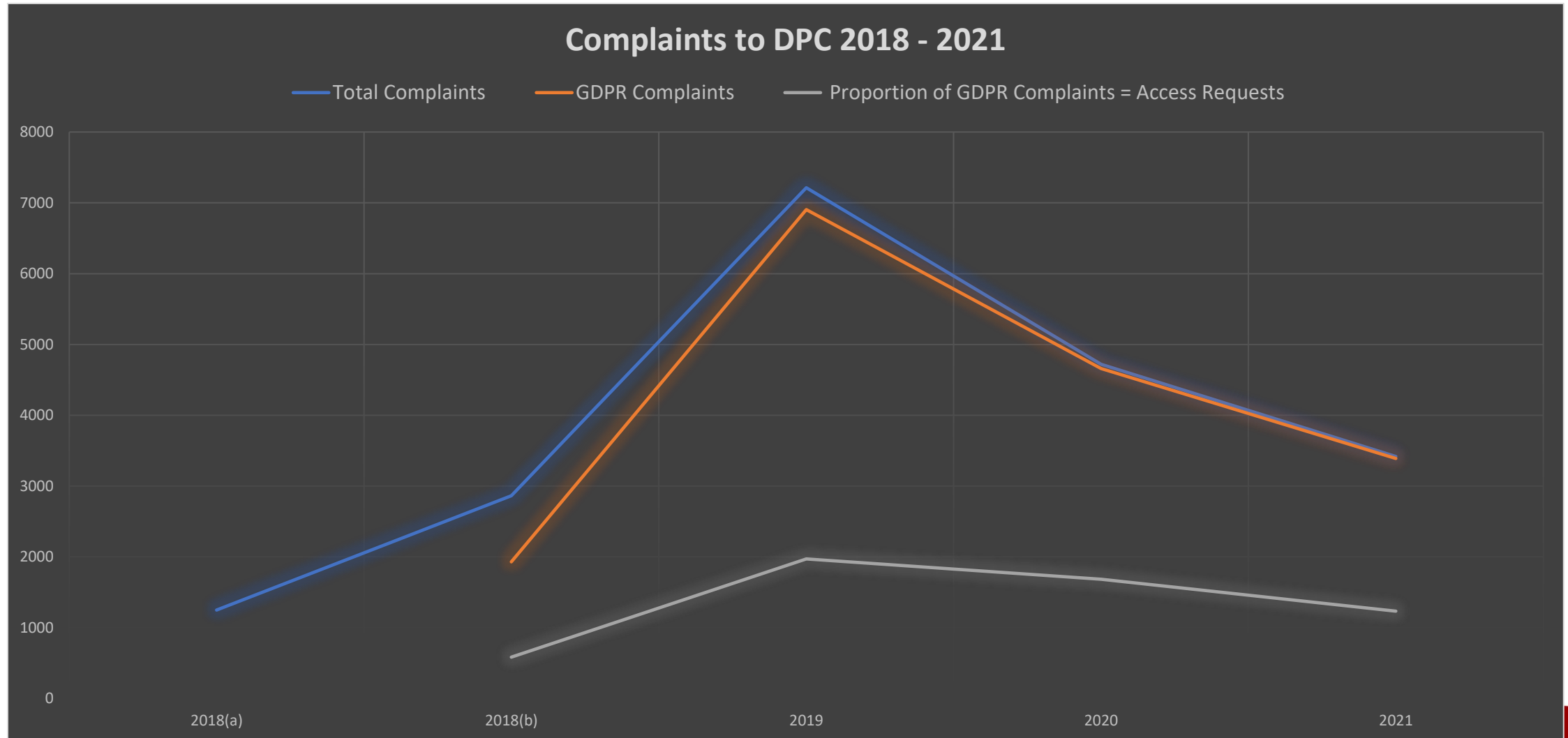
CalQRisk used by 400+ Regulated Organisations

- Financial Services Sector, Fund Administration, Credit Unions, Brokers, Charities, Sports Sector, Law Firms, Leisure Sector, Education (Schools & Colleges), and Local Authorities / Public Sector
- They use CalQRisk to record and report on their Risk, Control, Compliance and Audit activity and much more

# Introduction

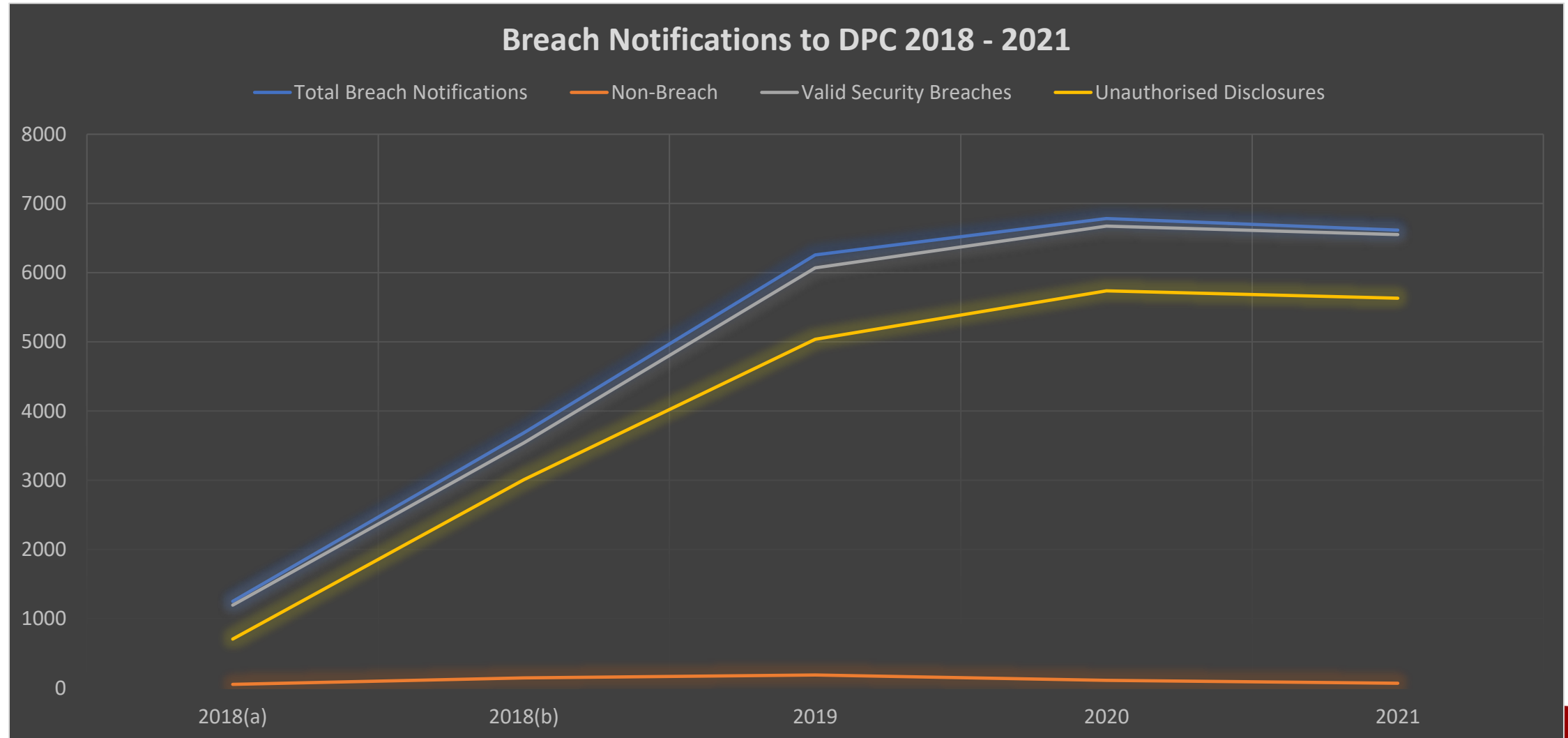


# Overview 2018-2022



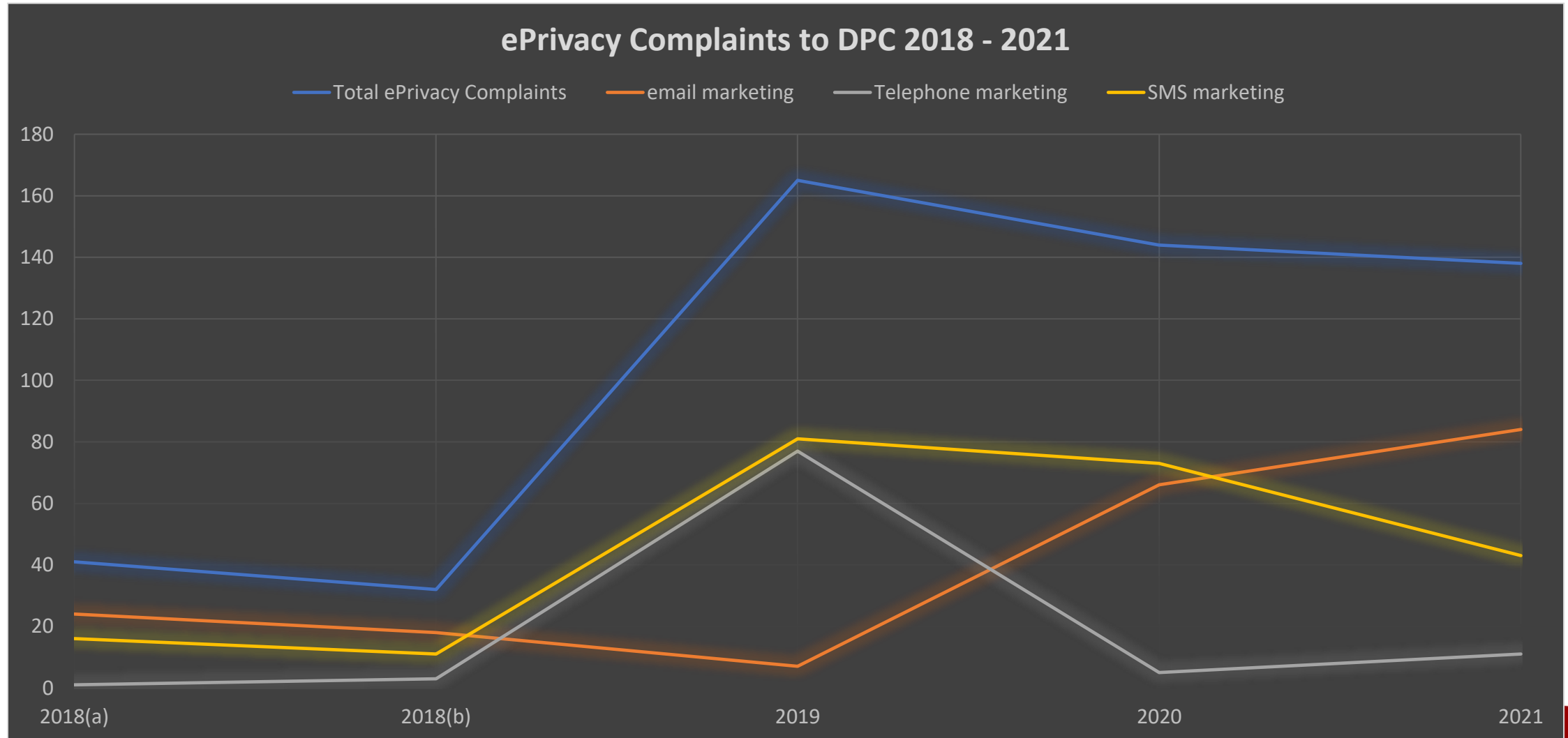
Source: DPC Annual Reports 2018 - 2021

# Overview 2018-2022



Source: DPC Annual Reports 2018 - 2021

# Overview 2018-2022



Source: DPC Annual Reports 2018 - 2021

# Overview 2018-2022

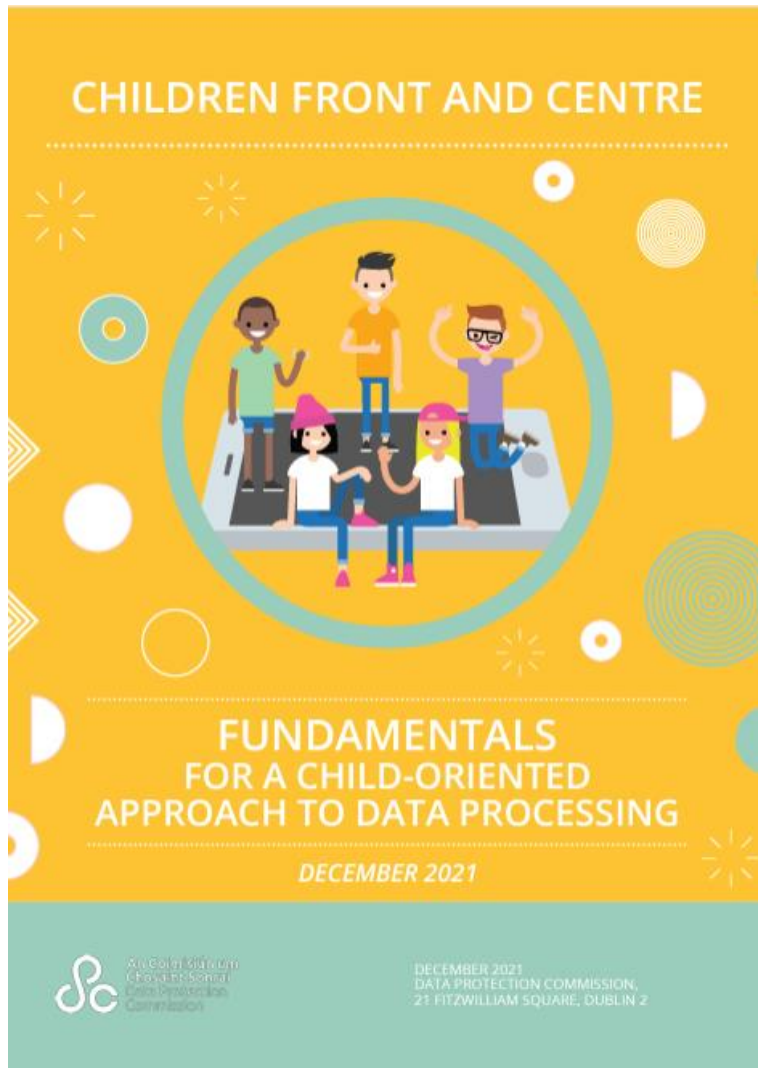
## Significant DPA Initiatives

Guidelines on the interplay with PSD2 and the GDPR, EDPB [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-062020-interplay-second-payment-services\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-062020-interplay-second-payment-services_en)

Fundamentals for a Child-Oriented Approach to Data Processing, DPC <https://www.dataprotection.ie/en/dpc-guidance/fundamentals-child-oriented-approach-data-processing>

Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, EDPB [https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition\\_en](https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en)

<https://www.irishtimes.com/opinion/letters/2022/06/02/garda-use-of-facial-recognition-technologies-unnecessary-and-disproportionate/>





## Significant Court Rulings

### **Doolin v The Data Protection Commissioner**

Issue: Further Processing of Personal Data

DPC, Circuit Court, High Court, Court of Appeal – Doolin successful

### **Data Protection Commissioner v Facebook Ireland Ltd (Schrems II)**

Issue: Schrems challenges legality of data transfers to USA that rely on Standard Contractual Clauses

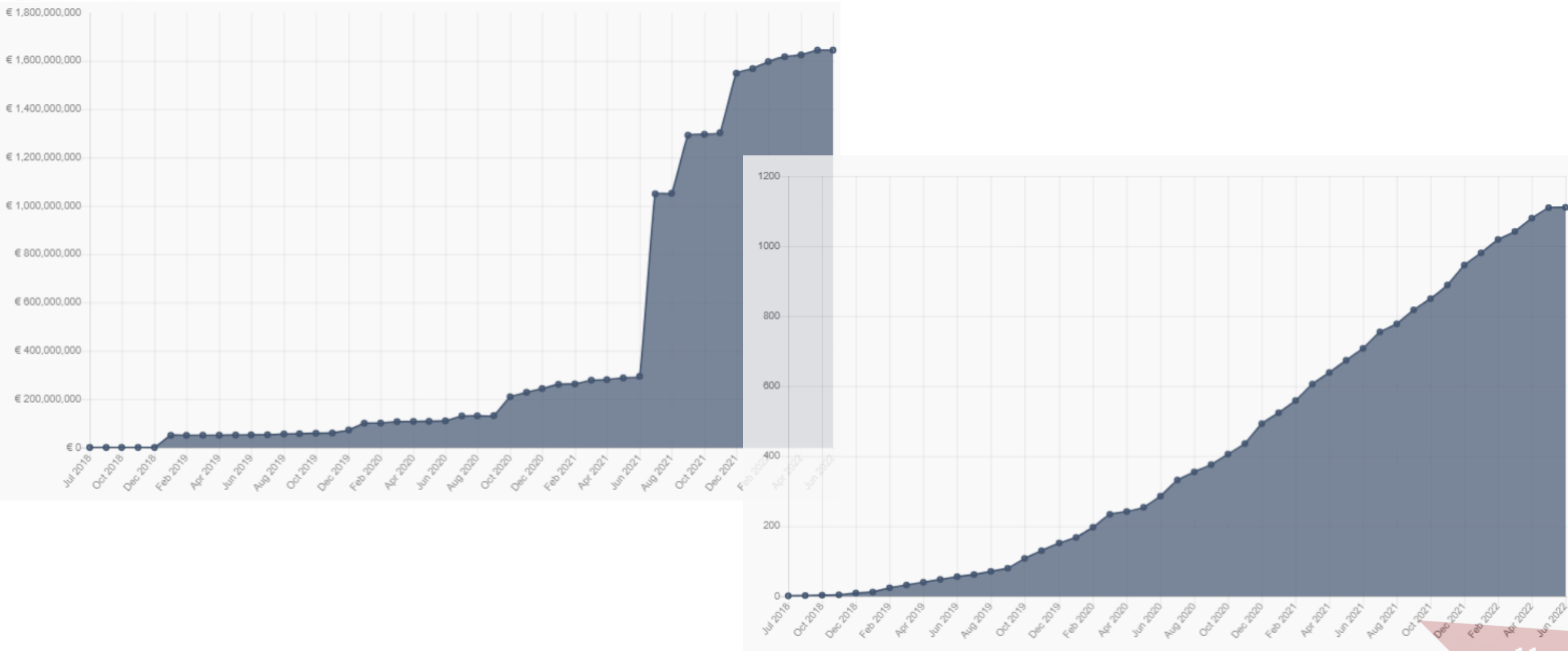
DPC, High Court -> CJEU (11 questions) – Validity of SCCs upheld but Privacy Shield declared invalid

### **Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH (Planet49 case)**

Issue: Consent to transfer of personal data to commercial third parties

Regional Court, Higher Regional Court, Federal Court of Justice -> CJEU (4 questions) -

# Cumulative Fines 2018 - 2022



## Significant Fines by Data Protection Authorities

1. Amazon €746m (CNPD)

[https://www.sec.gov/ix?doc=/Archives/edgar/data/0001018724/000101872421000020/amzn-20210630.htm#i5986f88ea1e04d5c91ff09fed8d716f0\\_103](https://www.sec.gov/ix?doc=/Archives/edgar/data/0001018724/000101872421000020/amzn-20210630.htm#i5986f88ea1e04d5c91ff09fed8d716f0_103)

2. WhatsApp €225m (DPC)

[https://edpb.europa.eu/system/files/2021-09/dpc\\_final\\_decision\\_redacted\\_for\\_issue\\_to\\_edpb\\_01-09-21\\_en.pdf](https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf)

3. Google LLC €90m (CNIL)













<https://www.cnil.fr/fr/cookies-la-cnil-sanctionne-google-hauteur-de-150-millions-deuros>

4. Facebook IRL €60m (CNIL)

<https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044840532>

5. Google IRL €60m (CNIL)

<https://www.cnil.fr/fr/cookies-la-cnil-sanctionne-google-hauteur-de-150-millions-deuros>

ETid	Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type
<input type="text" value="Filter Column"/>	<input type="text" value="Filter Column"/>		<input type="text" value="Filter Column"/>	<input type="text" value="Filter Column"/>		<input type="text" value="Filter Column"/>
ETid-778	 LUXEMBOURG	2021-07-16	746,000,000	Amazon Europe Core S.à.r.l.	Unknown	Non-compliance with general data processing principles
ETid-820	 IRELAND	2021-09-02	225,000,000	WhatsApp Ireland Ltd.	Art. 5 (1) a) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR	Insufficient fulfilment of information obligations
ETid-978	 FRANCE	2021-12-31	90,000,000	Google LLC	Art. 82 loi Informatique et Libertés	Insufficient legal basis for data processing
ETid-980	 FRANCE	2021-12-31	60,000,000	Facebook Ireland Ltd.	Art. 82 loi Informatique et Libertés	Insufficient legal basis for data processing
ETid-979	 FRANCE	2021-12-31	60,000,000	Google Ireland Ltd.	Art. 82 loi Informatique et Libertés	Insufficient legal basis for data processing
ETid-23	 FRANCE	2019-01-21	50,000,000	Google LLC	Art. 13 GDPR, Art. 14 GDPR, Art. 6 GDPR, Art. 5 GDPR	Insufficient legal basis for data processing
ETid-405	 GERMANY	2020-10-01	35,258,708	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
ETid-189	 ITALY	2020-01-15	27,800,000	TIM (telecommunications operator)	Art. 5 GDPR, Art. 6 GDPR, Art. 17 GDPR, Art. 21 GDPR, Art. 32 GDPR	Insufficient legal basis for data processing
ETid-1005	 ITALY	2021-12-16	26,500,000	Enel Energia S.p.A	Art. 5 (1) a), d) GDPR, Art. 5 (2) GDPR, Art. 6 (1) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 21 GDPR, Art. 24 GDPR, Art. 25 (1) GDPR, Art. 30 GDPR, Art. 31 GDPR, Art. 130 (1), (2), (4) Codice della privacy	Insufficient legal basis for data processing
ETid-58	 UNITED KINGDOM	2020-10-16	22,046,000	British Airways	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security
ETid-60	 UNITED KINGDOM	2020-10-30	20,450,000	Marriott International, Inc	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security
ETid-1098	 ITALY	2022-02-10	20,000,000	Clearview AI Inc.	Art. 5 (1) a), b), e) GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 15 GDPR, Art. 27 GDPR	Non-compliance with general data processing principles

# Adequacy Decisions

Switzerland

Faroe Islands

Japan

Canada (commercial organisations)

Andorra

United Kingdom

Argentina

Israel

Republic of Korea

Guernsey

Uruguay

Isle of Man

New Zealand

Jersey

# Brexit Key Dates

- 19/03/2018 EU & UK agree transition phase
- 25/11/2018 Draft withdrawal deal agreed
- 29/10/2019 EU approves postponing Brexit date
- 31/12/2020 Transition period ends
- 01/01/2021 EU-UK Trade and Cooperation Agreement begins, and  
**UK GDPR in force**
- 28/06/2021 EU approves adequacy decisions for transfers under GDPR & LED**
- 27/06/2025 UK Adequacy expires under 'Sunset Clause', unless extended

Today minimal divergence between EU GDPR and UK GDPR

- adequacy decision in place
- most data can flow from EEA to UK without additional safeguards

UK Data Protection Reform Bill forthcoming:

- adequacy at risk in the future
- 'Frozen GDPR' will apply to 'Legacy Data' if UK adequacy decision is lost

# New Compliance Risk?

UK Organisations may also be subject to EU GDPR... and vice versa

- **Under Article 3(1)** This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the [\[territory\]](#), regardless of whether the processing takes place in the [\[territory\]](#) or not.
- **Article 3(2)...**



# Territorial Scope - Article 3

**EU GDPR 3(2)** “... Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to...”

**UK GDPR 3(2)** “... Regulation applies to the [relevant] processing of personal data of data subjects who are in the United Kingdom by a controller or processor not established in the United Kingdom where the processing activities are related to...”

the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the [territory].

**OR**

the monitoring of their behaviour as far as their behaviour takes place within the [territory].

# The “Forgotten” Article – A.27 Representative

Establishment of DC / DP	Location of Article 3(2) processing		
	EU / EEA Only	UK Only	EU & UK
EU / EEA		UK Representative	UK Representative
UK	EU Representative		EU Representative
Outside EU / EEA & UK	EU Representative	UK Representative	EU & UK Representative

**Designation must be in writing**

**Obligation does not apply to:**

processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing;

**or**

a public authority or body.

# The Collapse of Privacy Shield

6<sup>th</sup> October 2015 – Safe Harbour ruled invalid by ECJ in Maximillian Schrems v Data Protection Commissioner ('Schrems I')

16th July 2020 - DPC v Facebook Ireland Ltd, Maximillian Schrems ('Schrems II'), ECJ ruled Privacy Shield is invalid.

25<sup>th</sup> March 2022 - Agreement in Principle between EU & US on a new Trans-Atlantic Data Privacy Framework

*This failed twice before. What we heard is another 'patchwork' approach but no substantial reform on the U.S. side. Let's wait for a text but my [first] bet is it will fail again. Max Schrems*



Source: Leman Solicitors 2016



Source: Evelyn Hockstein / Reuters 2022

# Cross-Border Transfers & SCCs

EU Commission's Implementing Decision on Standard Contractual Clauses (SCCs) published on 4<sup>th</sup> June 2021

New SCCs will replace those developed under the Data Protection Directive

In force since 27<sup>th</sup> June 2021

Since September 2021, old SCCs can no longer be used in new agreements.

Where old SCCs are already in place, transition period ends on 27<sup>th</sup> December 2022

[https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en)

# What is Appropriate?

If TOMS was a vehicle...

And you wanted to get from A to B

- A Ford Fiesta                      will get you there,
- A Bullet proof van              if you are transporting large amounts of cash
- A 40 foot truck                  if you are transporting furniture

# Information Security

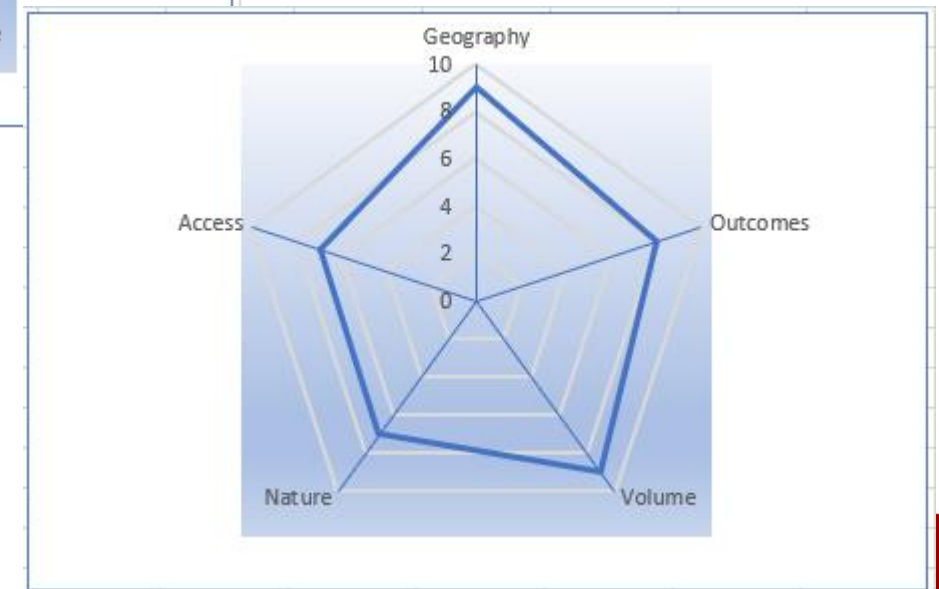
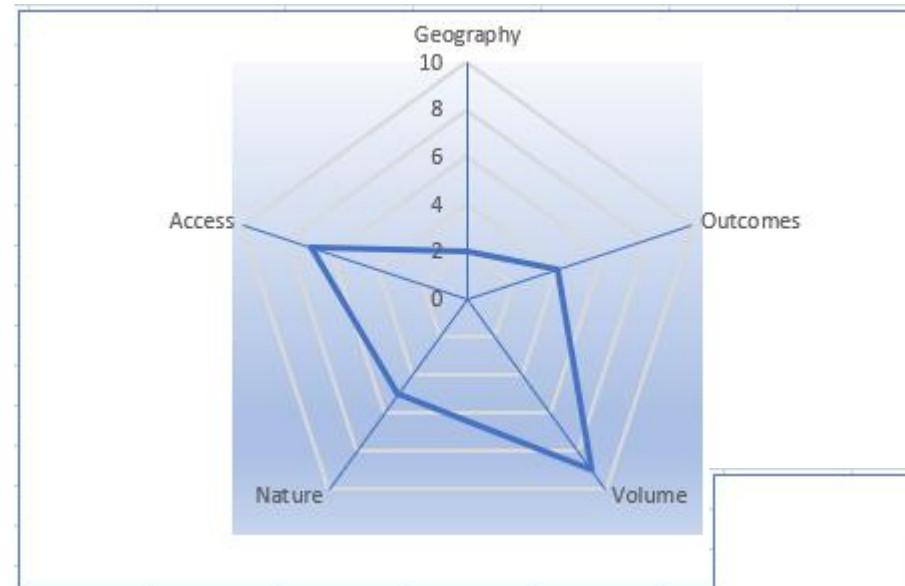
## C I A

- Confidentiality
- Integrity
- Availability



# Nature, Scale and Complexity

- Geography
- Outcomes
- Volume
- Nature
- Access



# Minimum Expectations

- An information security policy
- A data retention policy
- Assigned responsibilities
- Least privilege access policy
- Backup data on a daily basis
- Security by design... in any software application
- Robust Change management
- Encrypt personal data
- Encrypt data in transit
- Encrypt backup data, store off the network.
- Incident Response Plan
- Data Restore
- Test your measures
- Train your employees

**Lived Organisational Processes**



# Other Measure to Consider

- Information Classification
- Multi Factor Authentication
- Failover / Alternative systems
- Uninterruptible Power Supplies
- Generators
- Testing the Restore process
- Asset Inventory
- Penetration testing, incl vulnerability scanning
- Employee screening... reference checks
- Data destruction policy
- Equipment disposal policy / procedure
- Access Control Review on a quarterly basis

# What Next?

Long awaited ePrivacy Regulation – not expected any time soon

## European Data Strategy

- Data Governance Act
- A Single Market for Data
- Data Act

## EU Artificial Intelligence Act

## UK Reform – one to watch

## International Data Transfer Mechanisms

<https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation>

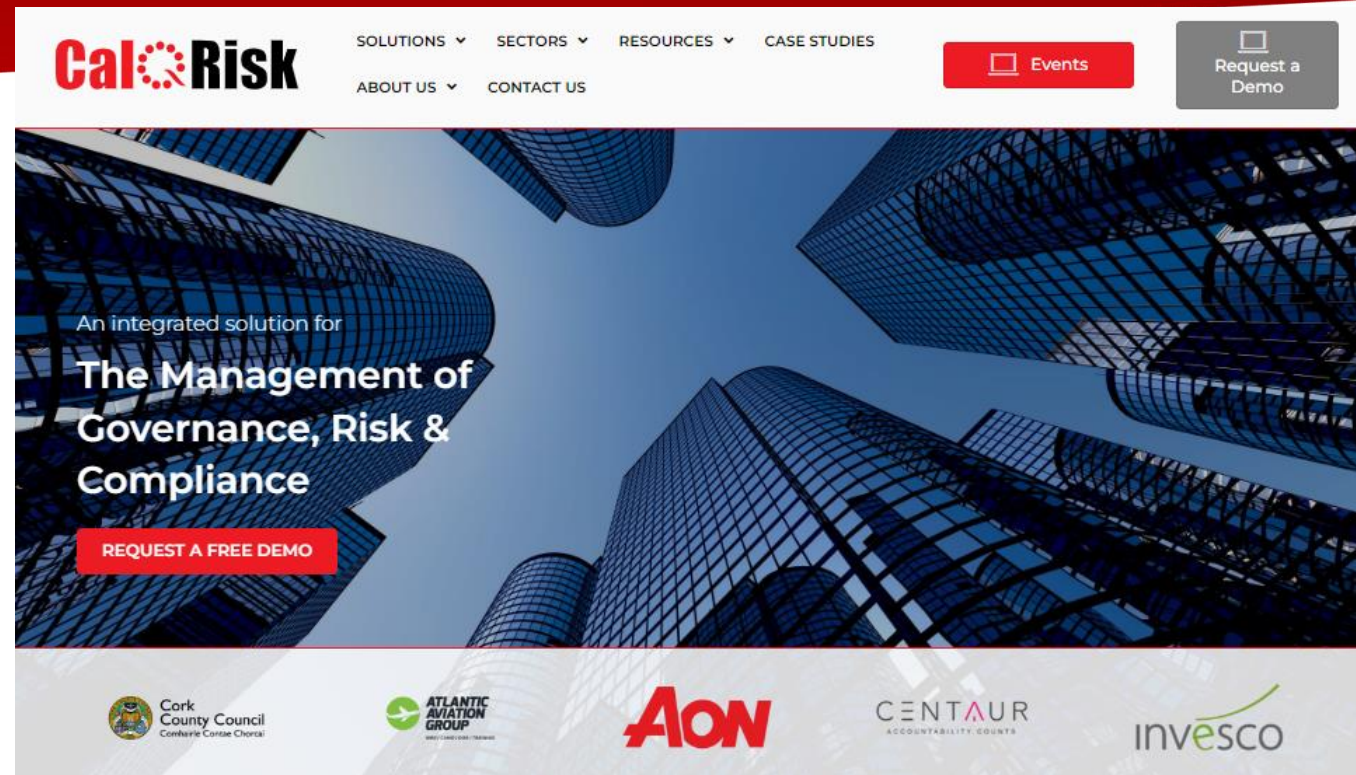
[https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy\\_en#:~:text=The%20European%20data%20strategy%20aims,businesses%2C%20researchers%20and%20public%20administrations](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en#:~:text=The%20European%20data%20strategy%20aims,businesses%2C%20researchers%20and%20public%20administrations)

[https://www.youtube.com/watch?v=9oYpf0AzD8s&ab\\_channel=PublicationsOfficeoftheEuropeanUnion](https://www.youtube.com/watch?v=9oYpf0AzD8s&ab_channel=PublicationsOfficeoftheEuropeanUnion)

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>



# Q & A



For articles and other resources, visit our website at <https://www.calqrisk.com>

Email us at [fkiely@calqrisk.com](mailto:fkiely@calqrisk.com), [gjoyce@calqrisk.com](mailto:gjoyce@calqrisk.com)

Next Webinar, June 15th at 10:30 Fundamentals of Good Governance for NGBs & LSPs