



GDPR One Year On

Cédric Burton

*Partner & Global Co-Chair,
Privacy and Cybersecurity*



Agenda

- GDPR One Year: guidance, complaints, and enforcement trends
- A few selected advanced topics:
 - Territorial scope of the GDPR
 - Personal, pseudonymized, and anonymized data
 - Chain of data processing: a few issues
 - Data transfers: new tools, ongoing challenges, Brexit
 - Online tracking, cookies, and real time bidding

EDPB Guidance & Documents

- Derogations for data transfers
- Territorial scope of the GDPR
- Processing necessary for the performance of a contract in the context of online services
- Code of conduct and certification
- Opinions/letters on ePrivacy, GDPR implementation, Brexit, BCRs, interaction between the GDPR and the Clinical Trial Regulation and PSD2, Japan, Privacy Shield
- Data protection impact assessments

Enforcement

- **375,000+** registered DPOs
- **90,000+** data breach notifications
- **95,000+** complaints
- **400+** cross-border investigations
- Approx. **EUR 57,000,000** of fines

GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook

May 25, 2018



Netflix, Spotify & YouTube: Eight Strategic Complaints filed on "Right to Access"

Jan 18, 2019



A test by noyb shows structural violations of most streaming services. In more than 10 test cases noyb was able to identify violations of Article 15 GDPR in many shapes and forms by companies like Amazon, Apple, DAZN, Spotify or Netflix. noyb has filed a wave of 10 strategic complaints against 8 companies today.

ACTION DE GROUPE CONTRE LES GAFAM

Les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) nous font payer leurs services avec nos libertés.

Our complaints against Acxiom, Criteo, Equifax, Experian, Oracle, Quantcast, Tapad

It creeps us out.
That's why we are taking action to hold them to account.



PAHOPTYKON FOUNDATION



Google

iab.

<https://noyb.eu/4complaints/>
<https://gafam.laquadrature.net/>

Wilson Sonsini Goodrich & Rosati, LLP



A few Trends

Complaints

- A limited number of high-profile complaints
- Consumer (organization) activism expected to grow further
- Complaints drive enforcement (consent, transparency, rights, and breaches)
- Primarily B2C complaints
- Increase of complaints by 40-60% depending on data protection authorities (“DPAs”)
- About 50% of the complaints have been closed

Investigations

- Generally not much visibility
- DPAs are still getting up to speed
- Expect the number of investigations to increase
- Proactive vs reactive

Fines & Litigation

- Amount of fines stays relatively low
- Expect new fines over the summer
- Litigation is still minimal
- Effects of enforcement by “regular courts”?
- “Transnational effect” of case-law?
- CJEU case-law

Territorial Scope

**Controller
established in the EU**



processing personal data
in the context of that EU
establishment



Regardless of
who the data
relates to

**Processor
established in the EU**



- *Establishment* means a real and effective activity exercised through stable arrangements in the EU.
- EU processor subject to the GDPR needs to enter into a “light” data processing agreement with controllers not subject to the GDPR.
- A non-EU controller that uses an EU processor does not automatically become subject to GDPR.

Territorial Scope

Israeli
company



Offer goods & services

Monitor behavior



Use of an EU
language or
currency

Use of an EU
domain name

Delivery of goods
to EU countries

Facilitation of
access to website
by EU based
individuals

Behavioral
advertisement

Online tracking

Market surveys

Geo-localization

Regular reporting

Territorial Scope

Israeli
company



Process payroll of EU employees

Monitor use of IT or conduct employees geo-tracking

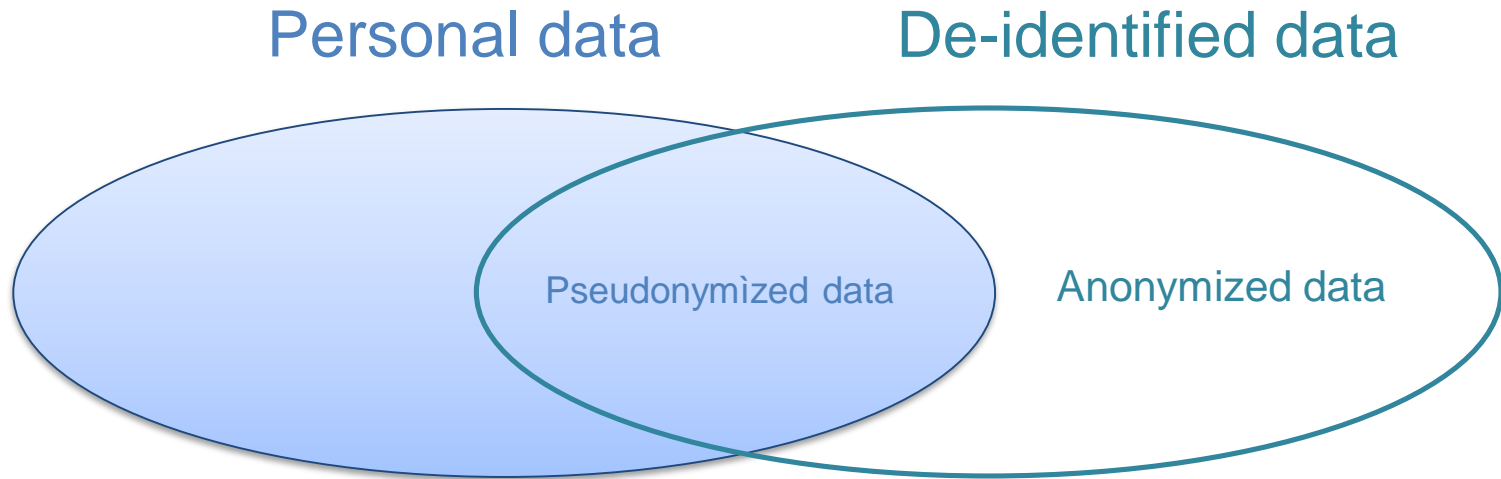
Provide a mobile app in the EU

Provide cloud storage to EU individuals or EU companies

Collect business contact details in the B2B context

- Uncertainty as to application to processors (statutory vs. contractual)
- Obligation to appoint a representative (liability, market?)

Personal, pseudonymized, and anonymized data




- Personal data is a very broad concept; anonymized data falls outside the scope of the GDPR
- UIDs: online IDs, cookies IDs, IP address, advertising IDs
- One way-hash
- One party hosting two segregated databases?
- How can you achieve anonymization?

Personal, pseudonymized, and anonymized data

- **Recital 26 GDPR**

To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.

To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

 We therefore have to test that we have taken into account **“all means”** **“reasonably”** **“likely”** **to be used by “controller”** or any **“other person”**.

- Difficult, but not impossible to reach the high threshold for anonymization.

Personal, pseudonymized, and anonymized data

WP29 opinion on anonymization

Singling out

What is the likelihood that an individual be singled out?

Linkability

How likely is it to link the records of the same individual?

Inference

How likely is it to draw inferences about individuals?

Is the process sufficiently robust for identification to be “reasonably” impossible?

Chain of Data Processing

Controller



Processor



Sub-Processor

- **Controller to Processor**

- Mandatory data processing agreement between the controller and processor
- The contract must oblige the processor to only process data on the instruction of the controller and to assist the controller to comply with the GDPR
- Article 28 GDPR lists the provisions that must be included in data processing agreements

- **Processor to Sub-Processor**

- Mandatory data processing agreement between the processor and sub-processor
- The contract must impose on the sub-processor the same obligations as are imposed on the processor by the controller

Chain of Data Processing

Sub-processing

Need to obtain the controller's prior written authorization

Specific authorization:

Controller must authorize each sub-processor separately

- Best avoided for processors, but sometimes controllers insist on the specific authorization regime

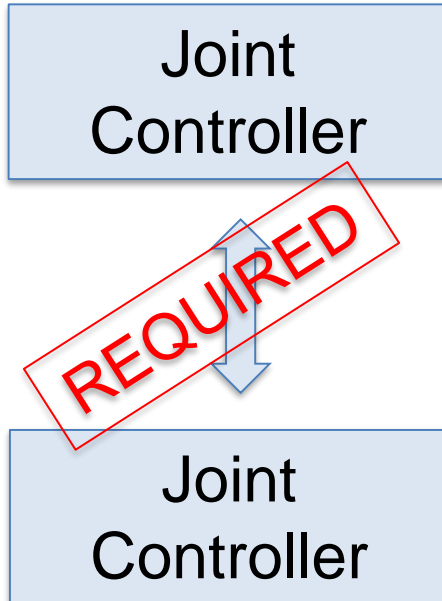
General authorization:

Controller gives a general authorization for sub-processing, but:

- Controller must be informed of any replacement or addition of a sub-processor; and
- Controller may object to the sub-processing.

- More flexible for processors
- Processors to consider creating a tool to update list of sub-processors whenever there is a change and inform customers of the change

Chain of Data Processing



- **Joint Controllers**

- Joint controllers are those who *jointly* determine the purposes and the means of the processing
- The GDPR requires a data processing agreement between joint controllers
- The agreement must determine the respective roles and responsibilities of the joint controllers
- Article 26 GDPR lists the provisions that must be included in the data processing agreement (e.g., who is to provide notice to individuals etc.)

Chain of Data Processing

Independent
Controller

NOT
REQUIRED

Independent
Controller

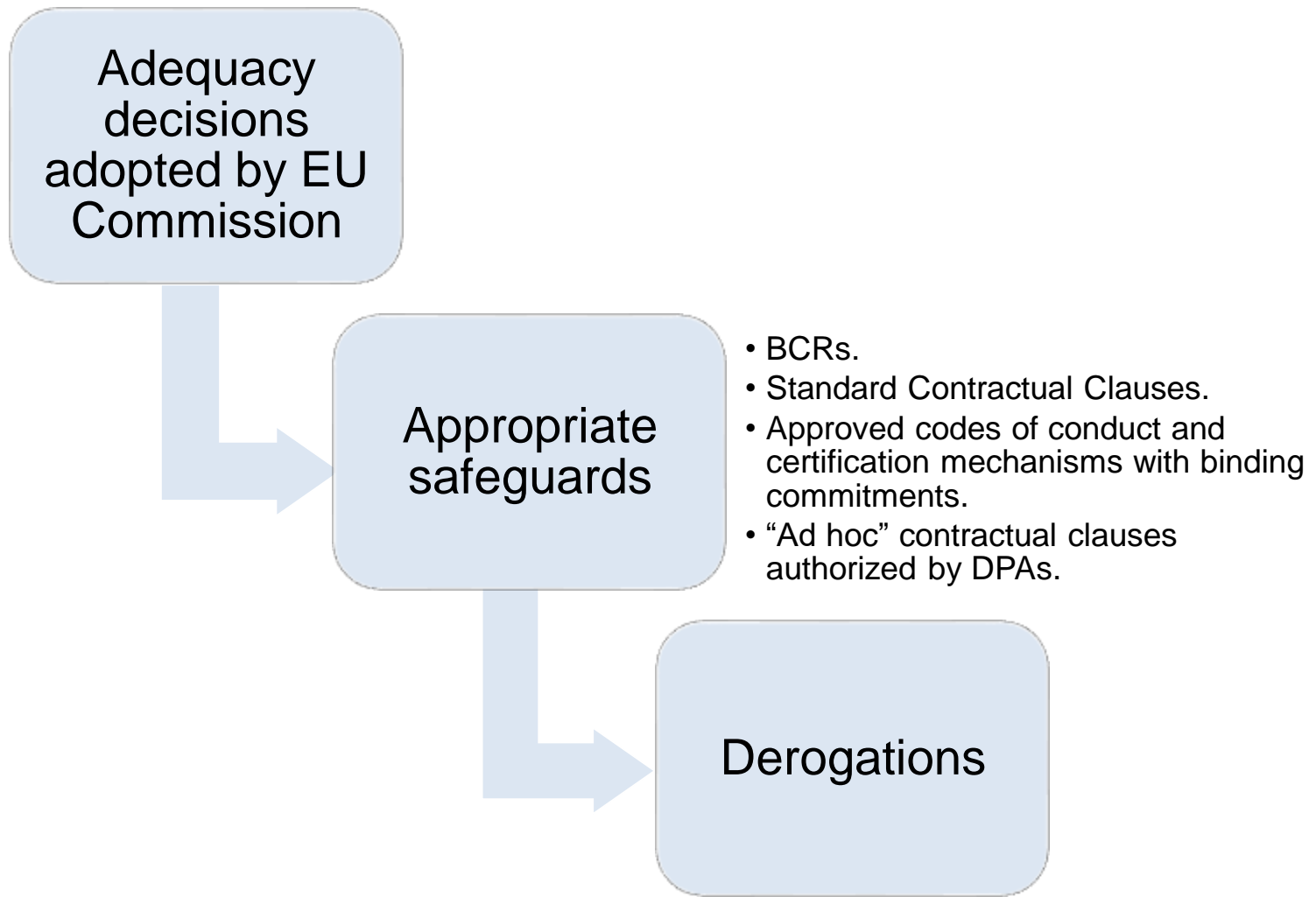
- **Independent Controllers**

- Independent controllers process the data each for their own purpose (i.e., they do not determine the purposes and the means of the processing *jointly*)
- The GDPR does not require a data processing agreement between two independent controllers, but companies tend to enter into such contracts as best practice
- Most companies try to avoid joint controllership (as it involves joint liability); however, there is a trend towards joint controllership (e.g., Facebook Fan Page decision)

Chain of Data Processing

- **Define roles and responsibilities**
 - Separate controllers, joint-controllers?
 - Push towards joint-controllership; but exact meaning is unclear.
- **Carve out for controller activities?**
 - Use of personal data for a service provider's own purposes, such as internal analytics, product development or fraud prevention & monitoring.
 - De-identification as an option?
- **Data controllers without contact with individuals**
 - How to provide notice?
 - ▶ What constitutes appropriate notice is still a moving target.
 - How to comply with individuals rights?
 - How to obtain consent?
 - Contractual representations are not enough as such.
- **Be accountable:** focus on legitimate interests analysis and DPIAs

International Data Transfers



International Data Transfers

	Scope	Legal certainty	Burden	
BCRs	<ul style="list-style-type: none"> Intra-group transfers Flexible Regulator approved 	<p>High (GDPR Art. 47)</p>	<ul style="list-style-type: none"> High upfront Low ongoing 	<hr/> <p style="text-align: center;">Data Protection Directive (Arts. 25, 26)</p> <ul style="list-style-type: none"> Transfers permissible only if third country ensures adequate level of protection <i>or</i> derogation applies Controllers responsible for compliance <div style="text-align: center; margin: 20px 0;"> </div> <hr/> <p style="text-align: center;">General Data Protection Regulation (GDPR) (Arts. 44-50)</p> <ul style="list-style-type: none"> Similar but more detailed transfer regime Controllers <i>and</i> processors responsible for compliance
Codes of Conduct/Seals	<ul style="list-style-type: none"> Sector/company specific New mechanisms must be developed Seals valid for up to 3 years; option to renew 	<p>Likely High (GDPR Arts. 40-43)</p>	<ul style="list-style-type: none"> High upfront Low ongoing 	
Commission Adequacy	<ul style="list-style-type: none"> Limited to countries recognized as providing adequate protection 	<p>High</p>	<ul style="list-style-type: none"> Low 	
Derogations (e.g., explicit consent, contractual performance)	<ul style="list-style-type: none"> Limited in scope Narrowly interpreted 	<p>Low to Medium</p>	<ul style="list-style-type: none"> Medium Documentation required 	
SCCs	<ul style="list-style-type: none"> Limited to contracting parties 	<p>Invalidation Risk</p>	<ul style="list-style-type: none"> Low Intensive maintenance 	
Privacy Shield	<ul style="list-style-type: none"> Limited to certain business EU to US transfers 	<p>Invalidation Risk</p>	<ul style="list-style-type: none"> High upfront Low ongoing 	

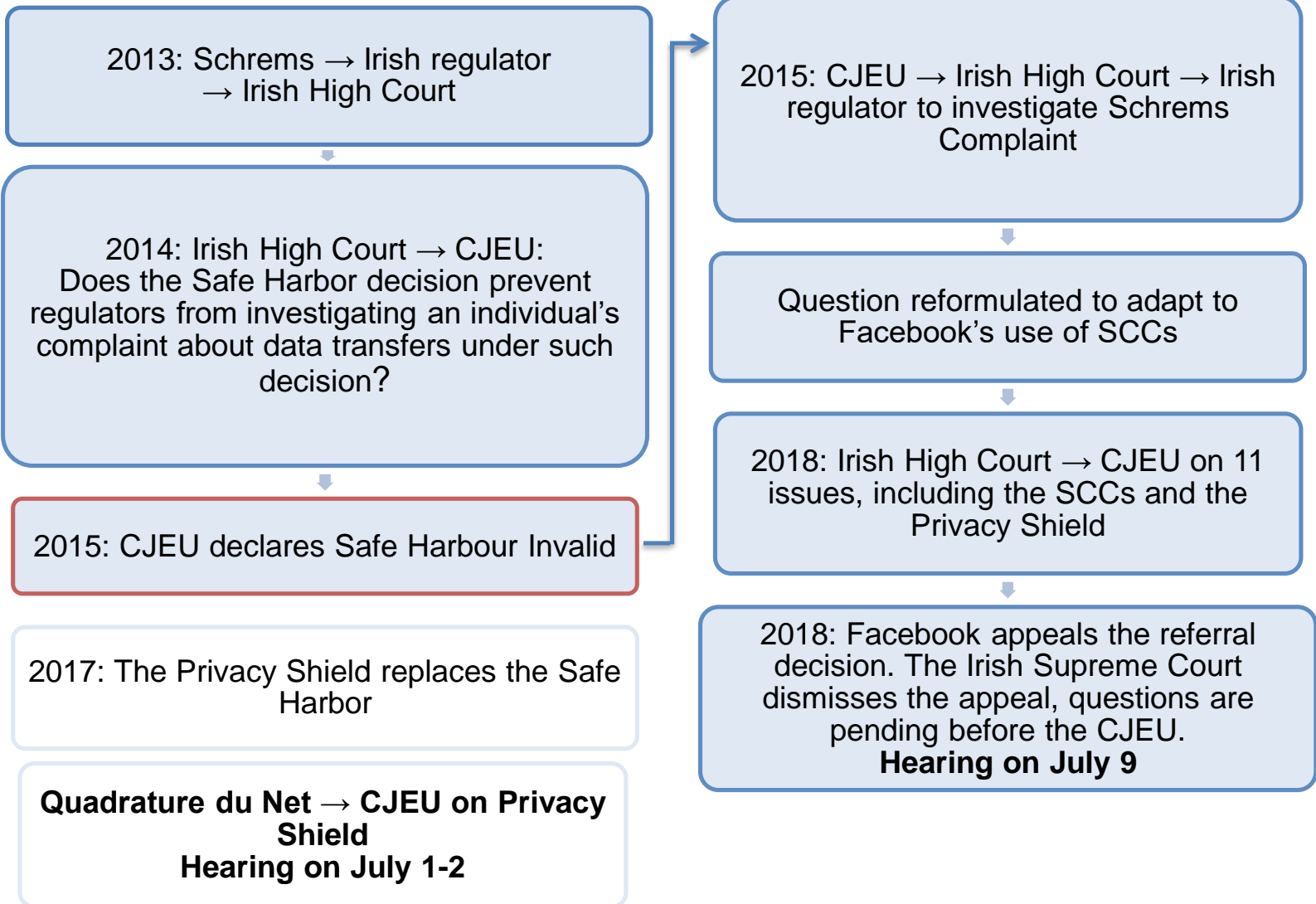
International Data Transfers

S
C
H
R
E
M
S

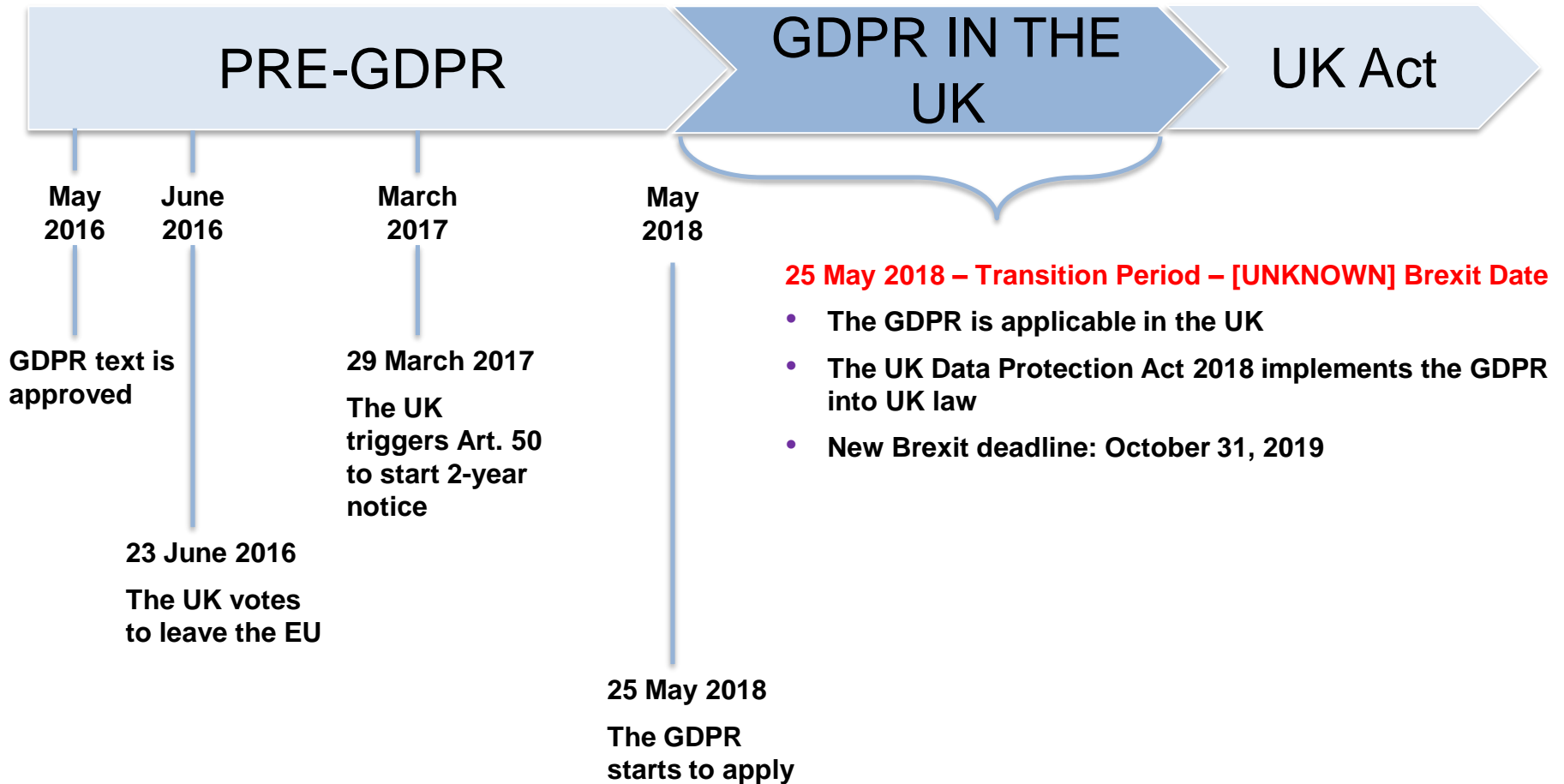
I

S
C
H
R
E
M
S

II



International Data Transfers: Brexit



Online tracking, cookies and real-time bidding



- **AG opinion in Fashion ID:** A website operator embedding a 3rd party plugin is jointly responsible for part of the processing, and has to provide notice and obtain consent.
- **AG opinion in Planet49:** Pre-ticked boxes are invalid and consent must be specific.
- **CNIL closed Teemo, Fidzup, Singlespot, and Vectaury** inquiries in October-November 2018, and February 2019.



Thank you! Questions?

Check our blog for news and updates

A promotional banner for 'THE WSGR DATA ADVISOR'. The banner has a light beige background with a decorative top border featuring a network of green and blue nodes connected by thin lines. The text is centered and reads: 'THE WSGR DATA ADVISOR' in a large, dark blue, sans-serif font. Below this, in a smaller, dark blue, sans-serif font, is 'Unique Insights on Privacy and Data Protection Worldwide'. Underneath that is the URL 'https://www.wsgrdataadvisor.com/' in a smaller, dark blue, sans-serif font. Below the URL is the text 'Enter your email address to subscribe to regular updates.' in a smaller, italicized, dark blue, sans-serif font. At the bottom of the banner, the WSGR logo is followed by the text 'Wilson Sonsini Goodrich & Rosati' and 'PROFESSIONAL CORPORATION' in a smaller, dark blue, sans-serif font.

THE WSGR DATA ADVISOR
Unique Insights on Privacy and Data Protection Worldwide
<https://www.wsgrdataadvisor.com/>
Enter your email address to subscribe to regular updates.

WSGR Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

Cédric Burton

Partner, Global Co-Chair Privacy and Cybersecurity

cburton@wsgr.com