Analysis of GDPR Enforcement Cases in the EU and Lessons for ASEAN

Kevin Shepherdson,
CIPP/E, CIPM, CIPP/A, CIPT, FIP, GDPR (Exin), GRCP

Lyn Boxall,
LLB, LLM, CIPP/E, CIPM, CIPP/A, FIP, GRCP, GRCA

William Hioe,
CIPP/E, CIPM, CIPP/A, CIPT, FIP, GDPR (Exin), GRCP

…provides practical solutions to current global privacy challenges/

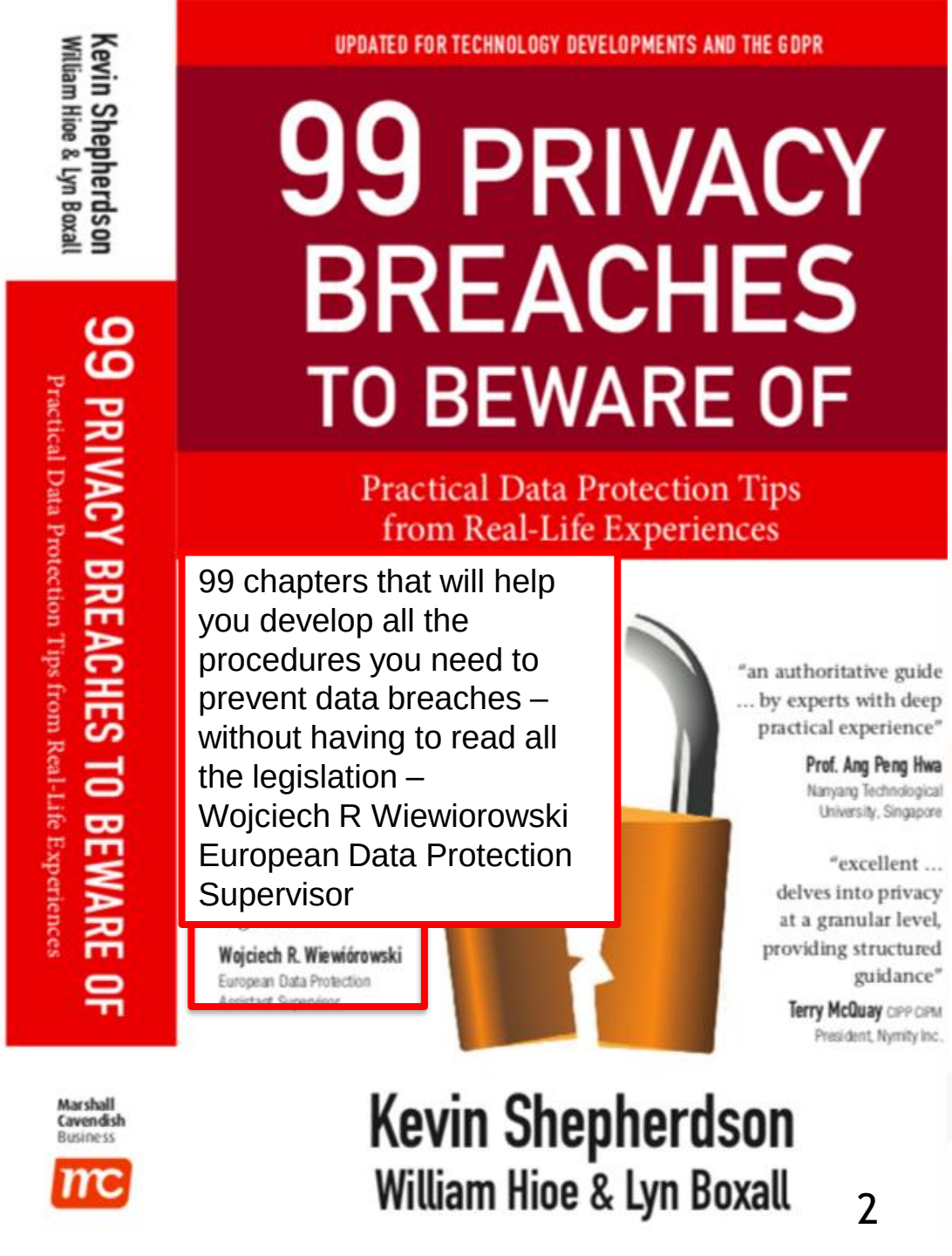
Patricia Poku,
Privacy Commissioner,
Ghana

Provides even more comprehensive coverage and analysis of data protection breaches and cases……..written for the layman and presented in a professional manner.....

Stephen Kai-yi Wong
Commissioner PCPD,
Hong Kong, China

For sure, this book you hold now will be remembered in the coming generations as another seminal work, contributing to the growing reservoir of knowledge on data privacy and security, and providing a solid foundation for the constant forward movement of global discourse.

Raymund Liboro
Commissioner, NPC
Philippines



Jim Campbell

IPP/US, Region Operations Manager, ANZ

Agenda

- Influence of GDPR on ASEAN
- Methodology of GDPR Analysis
- Insights of GDPR Enforcements in 2020
- Implications on ASEAN

GDPR established as de facto reference standard

General Data Protection Regulation (GDPR) in EU

New Upcoming Laws/ Amendments

Indonesia
PDP Bill
.

Thailand
PDPA

Philippines
DPA

India PDP Bill

China PI Security Specification / draft law

GDPR data protection principles being adopted and adapted for local context; concept of lawful/legal processing

GDPR established as de facto reference standard in ASEAN

GDPR Principles / Requirements are relevant to ASEAN from an operational if not regulatory perspective

	SG	MY	PH	TH	ID
Lawfulness of processing with **stricter consent requirements**	✔	✔	✔	✔	✔
Sensitive data / Special categories	NRIC	✔	✔	✔	✔
Requirements for DPO	✔	✔*	✔	✔	✔
Stricter requirements for processors	✔	✔*	✔	✔	✔
Data Protection Impact Assessment	Recommended	Recommended	Recommended	Recommended	Recommended
Data Protection by Design	Recommended	Recommended	Recommended	Recommended	Recommended
Data Breach notification		Recommended			
Records of processing (*INDO, TH)	Best practice	Best practice	Best practice		
Extra-territorial application (*PHI, TH)	N/A	N/A	*		N/A

**** Upcoming amendments***

New PDPA Amendments & GDPR

Singapore's PDPA

Consent Obligation

- Deemed consent* - disclosure based on *contractual necessity*

Consent Exception

- Consent Exception: *organisations are required to comply with other legal obligations*
- Consent Exception - Public interest, to participate in research, disclosed to any officer of a prescribed law enforcement agency
- Respond to an emergency that threatens the life, health or safety of the individual or another individual

- **Legitimate interests exception *and business improvement exception**

GDPR – Lawful Processing **

- **C**onsent
- **C**ontract Fulfilment / Performance
- **C**omply with legal obligation
- **I**nterests – Public, Public Authority performing task
- **I**nterests – Vital (life or death)
- **I**nterests – Legitimate business

* New PDPA amendments

** Comparison is purely based on operational perspective (not human rights)

Methodology & Scope

- Compilation from multiple sources across the Internet (include the GDPR enforcement tracker)
- Enforcement Cases are from 2018 (May 25) till Dec 2020.
- Analyses cover the following:
  - Amount of Fines (All numbers are in Euros)
  - Number of cases
  - By Articles Breached (Note that one case may have multiple articles breached)
  - All EU countries and those in the EEA and EFTA
- Accuracy is about 90% (total amount of fines match published reports +/- 5-10% delta)

European Union
27 Countries
(*but UK is included in the analysis because of the periods covered)*

European Economic Area
(EEA)
There are 30 EEA countries:

The 27 EU member states plus
Liechtenstein
Iceland
Norway

European Free Trade Association (EFTA).
Iceland
Liechtenstein
Norway
Switzerland

Supervision and Enforcement

Administrative fines

Up to €10,000,000 or 2% of total turnover (whichever is higher)

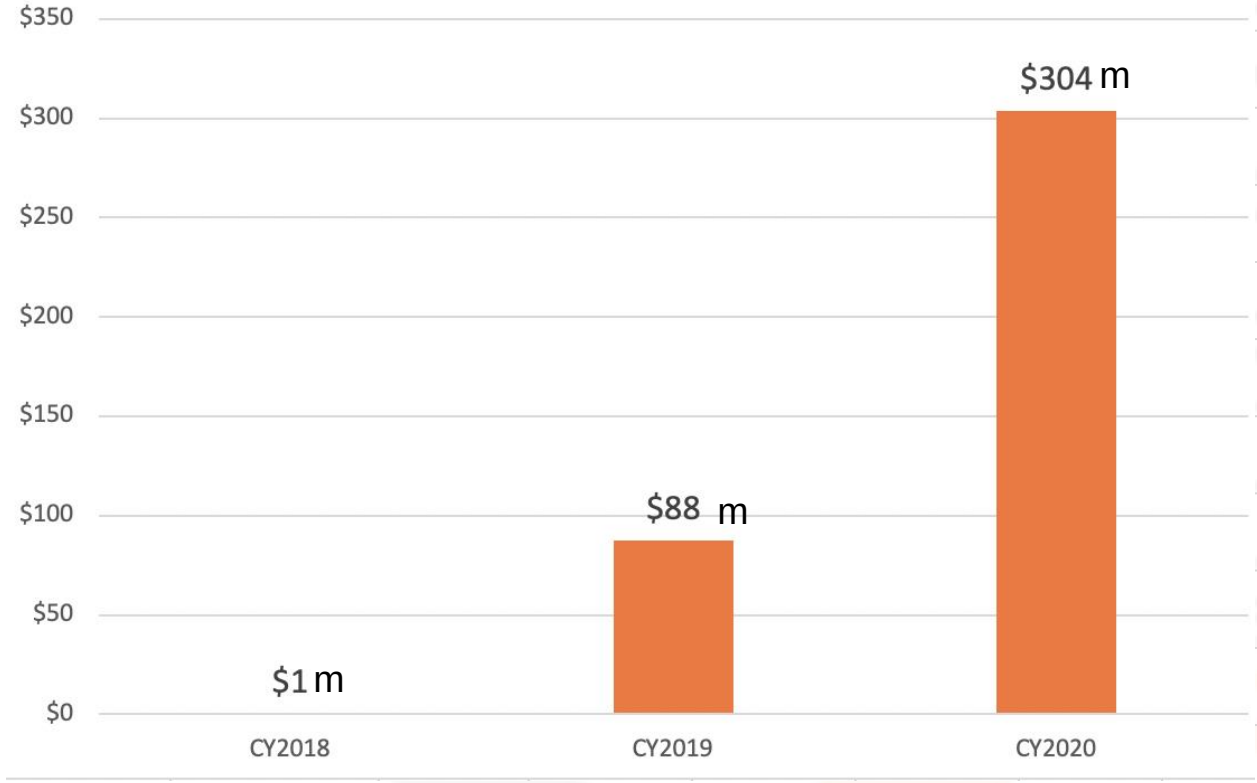
- ❑Art. 8 Conditions applicable to child's consent in relation to information society services
- ❑Art. 11 Processing which does not require identification
- ❑Art. 25 Data protection by design and by default
- ❑Art. 39 Tasks of the data protection officer
- ❑Art. 41 Monitoring of approved codes of conduct
- ❑Art. 42/43 Certification / Certification Bodies

Up to €20,000,000 or 4% of total turnover (whichever is higher)

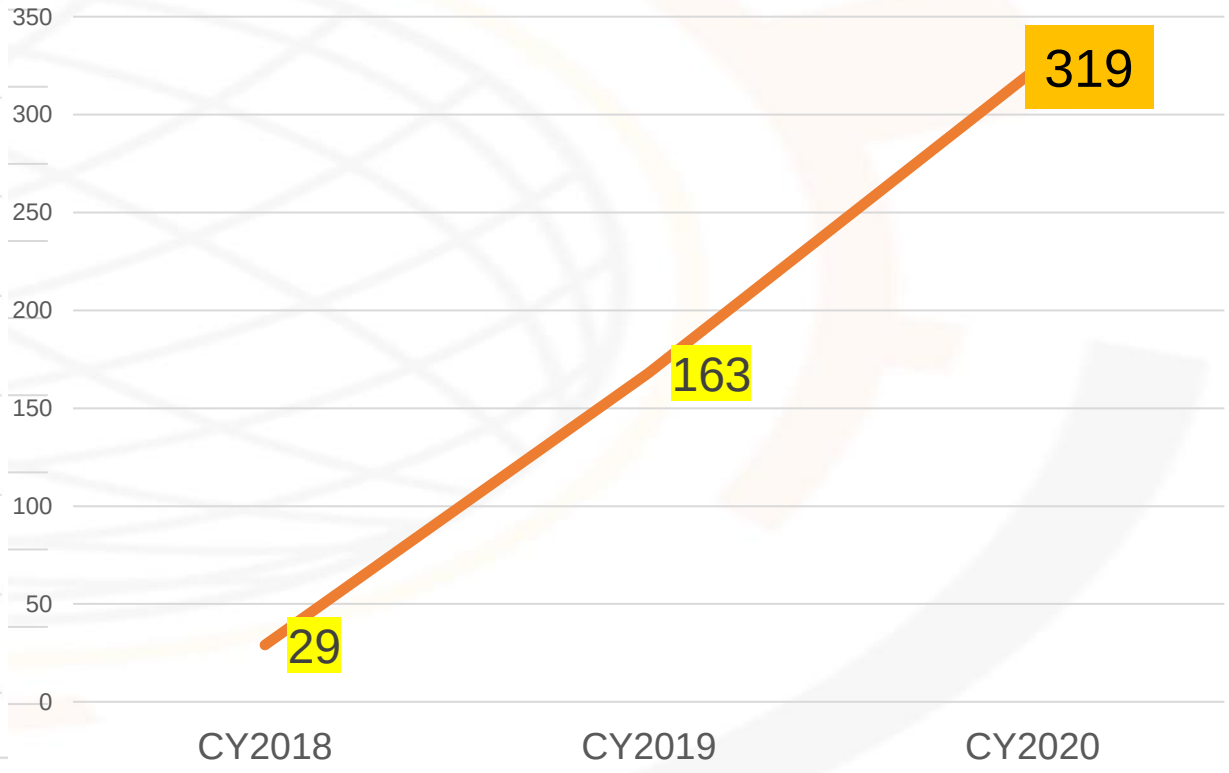
- ❑Art. 5 Principles relating to processing of personal data
- ❑Art. 6 Lawfulness of processing
- ❑Art. 7 Conditions for consent
- ❑Art. 9 Processing of special categories of personal data
- ❑Art. 12-22 Data subject's rights
- ❑Art. 44-49: The transfers of personal data to a recipient in a third country or an international organisation
- ❑Art. 58 non-compliance with an order from a SA

GDPR Fines and Cases had doubled in 2020

GDPR Enforcements 2018 - 2020
(Fines - EUR) – 393m EUR total fines

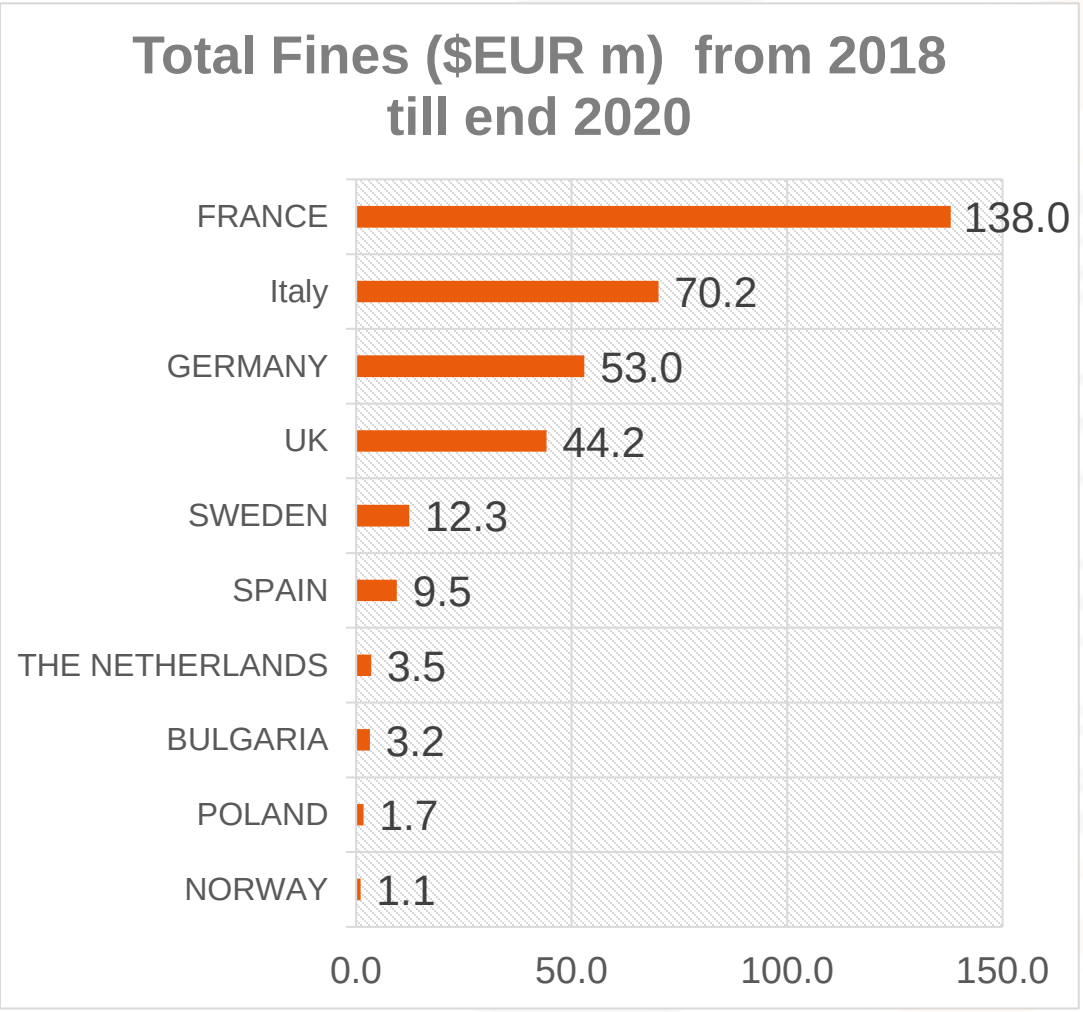


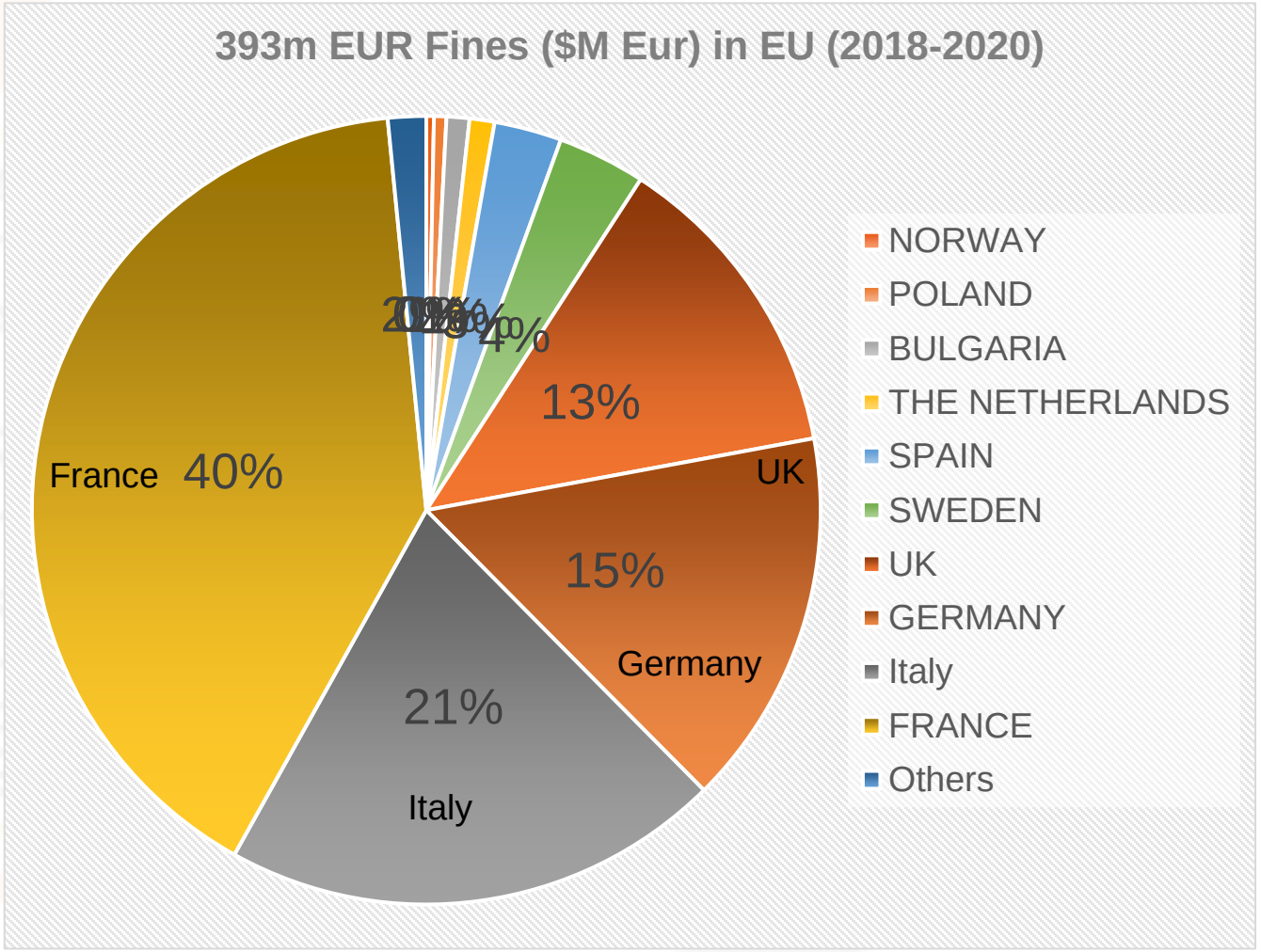
GDPR Enforcements 2018-2020
(# cases) – 511 cases



However, numbers by EU member states relatively small. Impact of COVID19 needs to be considered

Every member state in EU has enforced the GDPR since its inception except Luxembourg and Slovenia





Norway, Iceland and Isle of Man are the only 3 countries outside the EU (besides UK) which have also enforced the GDPR.

Spain is the country with most active enforcements

Country	CY2018	CY2019	CY2020	# of cases
SPAIN	7	31	133	171
ROMANIA		21	26	47
ITALY		3	36	39
HUNGARY	1	21	13	35
GERMANY	5	19	3	27
BELGIUM		6	14	20
BULGARIA	1	15	4	20
POLAND		5	11	16
SWEDEN		2	14	16
GREECE		5	7	12
NORWAY		2	10	12
CYPRUS		6	5	11
CZECH REPUBLIC	4	7		11
FRANCE		5	6	13
AUSTRIA	4	3	3	10
OTHERS	**7**	13	31	51
Number of enforcement cases	29	163	319	511

- Spain has total of 171 enforcements with 133 in 2020 (or 42% of total) .
- Note that there have only been a handful of enforcements cases in the individual member states.
- As comparison, SG PDPC Enforcement cases from 2016-2020
  - 162

18 companies have been fined >1m EUR

Controller/Processor. (2018 to 2020)	Country	Sum of Fine (EUR)	# of cases
Google Inc.	FRANCE	$150,000,000	2
Amazon	FRANCE	$35,000,000	1
H&M Hennes & Mauritz Online Shop A.B. & Co. KG	GERMANY	$35,258,708	1
TIM (telecommunications operator)	ITALY	$27,800,000	1
British Airways	UNITED KINGDOM	$22,046,000	1
Marriott International, Inc	UNITED KINGDOM	$20,450,000	1
Wind Tre S.p.A.	ITALY	$16,700,000	1
Deutsche Wohnen SE	GERMANY	$14,500,000	2
Vodafone Italia S.p.A.	ITALY	$12,251,601	1
Eni Gas e Luce	ITALY	$11,500,000	2
Banco Bilbao Vizcaya Argentaria, S.A.	SPAIN	$5,036,000	2
Google LLC	SWEDEN	$5,000,000	1
Capio St. Göran AB	SWEDEN	$2,900,000	1
Aleris Sjukvård AB	SWEDEN	$2,631,000	2
National Revenue Agency	BULGARIA	$2,628,100	2
Carrefour France	FRANCE	$2,250,000	1
Ticketmaster UK Limited	UNITED KINGDOM	$1,405,000	1
Allgemeine Ortskrankenkasse ('AOK') (insurance co)	GERMANY	$1,240,000	1
Vodafone España, S.A.U.	SPAIN	$912,000	20
Others		$23,994,557	467
TOTAL		$393,502,966	511

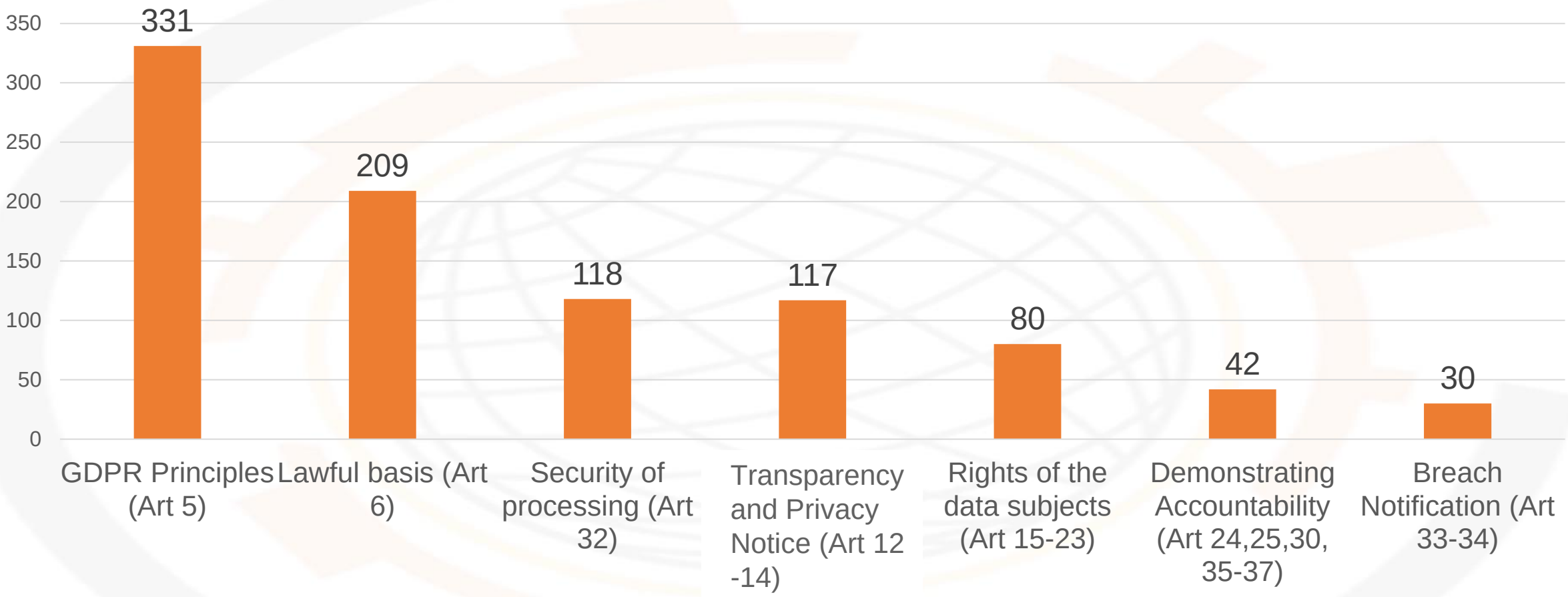
- From 2018 -2020, 20 companies had been fined >1m EUR, totaling about 93% of total fines of 393 m EUR
- Google has been fined in France and Sweden (>1m EUR)
- Vodafone has got 20 enforcement actions (totaling close to 1m EUR) during this period

Heavier fines were imposed in 2020 – 15 companies >1m EUR

		Sum of Fine				Count of Fine			
Controller/Processor	Country	CY2018	CY2019	CY2020	Total Sum of Fine	CY2018	CY2019	CY2020	Total Count of Fine
Google Inc.	FRANCE		$50,000,000	$100,000,000	$150,000,000		1	1	3
Amazon Inc.	FRANCE			$35,000,000	$35,000,000			1	1
H&M Hennes & Mauritz Online Shop A.B. & Co. KG	GERMANY			$35,258,708	$35,258,708			1	1
TIM (telecommunications operator)	ITALY			$27,800,000	$27,800,000			1	1
British Airways	UK			$22,046,000	$22,046,000			1	1
Marriott International, Inc	UK			$20,450,000	$20,450,000			1	1
Wind Tre S.p.A.	ITALY			$16,700,000	$16,700,000			1	1
Deutsche Wohnen SE	GERMANY		$14,500,000		$14,500,000		2		2
Vodafone Italia S.p.A.	ITALY			$12,251,601	$12,251,601			1	1
Eni Gas e Luce	ITALY		$11,500,000		$11,500,000		2		2
Banco Bilbao Vizcaya Argentaria, S.A.	SPAIN			$5,036,000	$5,036,000			2	2
Google LLC	SWEDEN			$5,000,000	$5,000,000			1	1
Capio St. Göran AB	SWEDEN			$2,900,000	$2,900,000			1	1
Aleris Sjukvård AB	SWEDEN			$2,631,000	$2,631,000			2	2
National Revenue Agency	BULGARIA		$2,628,100		$2,628,100		2		2
Carrefour France	FRANCE			$2,250,000	$2,250,000			1	1
Ticketmaster UK Limited	UK			$1,405,000	$1,405,000			1	1
Allgemeine Ortskrankenkasse ('AOK') (health insurance company)	GERMANY			$1,240,000	$1,240,000			1	1
Vodafone España, S.A.U.	SPAIN		$91,000	$821,000	$912,000		3	17	20

Top 7 Enforcement Areas (Articles) – (2018-2020)

Out of the 511 cases*



Note that the articles are based on those that have been breached in the enforcement cases

GDPR Principles, Lawful Basis, Security & Transparency

Articles *	CY2018	CY2019	CY2020	Grand Total	% of total cases
GDPR Principles (Art 5)	19	98	211	331	65%
Lawful basis (Art 6)	9	63	134	209	41%
Security of processing (Art 32)	8	35	75	118	23%
Transparency and Privacy Notice (Art 12-14)	6	32	77	117	23%
Rights of the data subjects (Art 15-23)	4	26	50	80	16%
Demonstrating Accountability (Art 24,25,30, 35-37)		16	26	42	8%
Breach Notification (Art 33-34)	2	10	18	30	6%
OTHERS	3	18	55	0	0%
Number of enforcement cases	29	163	319	511	
** Note: 1 case might have breach of multiple articles*					

- **65%** of all enforcement cases involve the breach of **GDPR principles**
- **41%** involve issues relating to **lawful basis**
- **23%** of all cases relate to issues relating to **transparency** and **rights of data subjects**

Country	GDPR Principles (Art 5)	Lawful basis (Art 6)	Security of processing (Art 32)	Transparency and Privacy Notice (Art 12-14)	Rights of the data subjects (Art 15-23)	Demonstrating Accountability (Art 24,25,30, 35-37)	Breach Notification (Art 33-34)	# Cases
AUSTRIA	9	6		5		1		10
BELGIUM	11	14		11	8	6		20
BULGARIA	13	13	4	3	3	4		20
CROATIA					1			1
CYPRUS	4	7	3		2		1	11
CZECH REPUBLIC	9	3	1		3			11
DENMARK	9	2	3		1		2	9
ESTONIA	1	2						2
FINLAND	3	3		3	1	2		5
FRANCE	11	2	6	11	5		3	11
GERMANY	10	8	5		5	3	4	27
GREECE	8	2	1	3	5	2		12
HUNGARY	28	15	5	14	14	7	6	35
ICELAND	2		2					2
IRELAND	2	1	1				2	4
ISLE OF MAN				1	1			1
ITALY	35	25	9	13	12	5	1	39
LATVIA	1	2		1	1			4
LITHUANIA	3		1				1	2
MALTA	2		1					1
NORWAY	8	5	8			1		12
POLAND	6	2	4	1		2	4	16
PORTUGAL	2		1	2	1			4
ROMANIA	14	10	27	6	7	3	3	47
SLOVAKIA	2	1	4		1			6
SPAIN	109	77	17	39	7	2	1	171
SWEDEN	21	5	9	1	1	4	2	16
NETHERLANDS	3	1	2	1	1			6
UK	2		4					4

Across EU… Top member states

For Transparency and Privacy Notice, Spain (39), Hungary (14), Italy (13)

For Rights of the Data Subjects Hungary (14), Italy (12), Belgium (8)

For Demonstrating Accountability Hungary (7), Belgium (6), Italy (5). Cases involve about half of member states

For Breach Notification, Hungary (6), Germany (4), Poland (4). Less than 10 member states have enforced breach notification

Integrity & Confidentiality, Data Minimisation, Lawfulness – Top GDPR Principles

GDPR Principles	CY2018	CY2019	CY2020	Grand Total
5. GDPR Principles (no details)	7	51	126	185
5 (1)f Integrity & Confidentiality	5	6	41	53
5 (1)c Data Minimisation	1	17	14	32
5 (1)a Lawfulness	3	14	10	27
5 (1)b Purpose Limitation	1	5	5	11
5 (2)Accountability		2	10	12
5 (1)e Storage Limitation		4	3	7
5 (1)d Accuracy	2	1	3	7
Number of enforcement cases	*29*	*163*	*319*	*511*

185 Enforcement cases did not state specific articles for GDPR principles

Not all EU member states have enforced the full GPDR principles

Country	5. GDPR principles	5 (1)f Integrity & Confi	5 (1)c Data Minimizatn	5 (1)a Lawfulness	5 (1)b Purpose Limitatn	5 (2) Accountability	5 (1)e Storage Limitation	5 (1)d Accuracy
AUSTRIA	3		1	5				
BELGIUM	7		3		1			
BULGARIA	5		1	5	2			
CYPRUS	2	1				1		
CZECH REPUBLIC	4	2	1	1			1	
DENMARK	4	2					3	
ESTONIA	1							
FINLAND	3							
FRANCE	7		2				2	
GERMANY	9		1					
GREECE	3		2	2	1			
HUNGARY	16		3	3	4		1	1
ICELAND		2						
IRELAND	2							
ITALY	25	4	1	5				
LATVIA	1							
LITHUANIA	1	1						1
MALTA	1		1					
NORWAY	5	3						
POLAND	3	2				1		
PORTUGAL	1	1						
ROMANIA	5	3	2	2	1			1
SLOVAKIA		2						
SPAIN	68	19	13	4	2			3
SWEDEN	5	8	1			7		
NETHERLANDS	3							
UK		2						
Grand Total	184	52	32	27	11	9	7	6

EXAMPLES of cases involving minimisation

[Spain, Feb 2020] Casa Gracio Operation

- The company used CCTV cameras in the premises of a hotel which also captured the public roads outside the hotel resulting in a violation of the principle of data minimisation.
- **Fine**: 6,000 euros

EXAMPLES of cases involving Accountability

[Italy, Nov 2020] Vodafone Italia S.p.A.

- Company **unlawfully processed personal data of millions of customers for telemarketing purposes**. The proceedings were preceded by hundreds of complaints from data subjects about unsolicited telephone calls, which led to an investigation by the data protection authority.
- This investigation revealed several violations of the data protection law, including the **violation of consent requirements and the violation of general data protection obligations such as accountability.**
- One of the main criticisms made by the Data Protection Agency was the **use of fake numbers to make promotional calls by the contracted call centers** (i.e. phone numbers not registered with the National Consolidated Registry of Communication Operators)
- Furthermore, **further violations could be found in the handling of contact lists purchased from external providers**.
- Finally, **security measures for the management of customer data were also considered inadequate.**
- **Fine**: 12,251,601 euros

Breach of lawful basis is about 40% of all cases

Consent, Legal Basis and Sensitive Data	CY2018	CY2019	CY2020	Grand Total
6. Lawful basis	9	63	134	206
4. Consent Specific/informed		1		1
7. Conditions for Consent	1	3	8	12
8. Child's consent			1	1
9. Special categories of data		7	10	17
Number of enforcement cases	*29*	*163*	*319*	*511*

Importance of having the right legal basis for processing in EU

Country	6. Lawful basis	7. Conditions for Consent	Art 4. Consent Specific/informed	8. child's consent	9. Special categories of data
AUSTRIA	6				1
BELGIUM	14	1			
BULGARIA	13				1
CYPRUS	7				3
CZECH REPUBLIC	3	1			
DENMARK	2				
ESTONIA	2				
FINLAND	3				
FRANCE	2		1		
GERMANY	8				
GREECE	2				
HUNGARY	15				
IRELAND	1				
ITALY	25	3			6
LATVIA	2				
NORWAY	5				
POLAND	2				1
ROMANIA	10	4			2
SLOVAKIA	1				
SPAIN	77	3		1	1
SWEDEN	5				1
NETHERLANDS	1				1
Grand Total	206	12	1	1	17

- Organisations getting into trouble for breach of consent (stricter requirements) – 12 cases in 5 member states
- EU member states enforcement of breach of special categories of data (17 cases)

EXAMPLES of cases involving unlawful legal basis

[Germany, Oct 2020] H&M

- The fashion company with seat in Hamburg operates a service center in Nuremberg. Here, according to the findings of the Hamburg data protection officer, since at least 2014, **private life circumstances of some of the employees have been comprehensively recorded and this information stored on a network drive**.
- In addition, according to the Hamburg data protection authority, **some supervisors also used the 'Flurfunk' [meaning to hear something through the grapevine] to acquire a broad knowledge of individual employees, for example about family problems and religious beliefs.**
- The information stored on the network drive was accessible to up to 50 managers of the company and was used, among other things, **to evaluate the work performance of the employees and to make employment decisions.**
- **The data collection became known due to a technical configuration error** in October 2019, according to which the data stored on the network drive was accessible company-wide for several hours. After the violation became known, the management apologized to the employees and offered monetary compensation. In addition, also further protective measures were introduced together with the data protection authority.
- **Fine**: 35,258,708 euros

EXAMPLES of cases involving unlawful legal basis

[Spain, Nov 2020] Telefonica Moviles Espana, S.A.U.

Processing of personal data of the data subject without sufficient legal basis. The company had issued several invoices to the data subject and collected invoice amounts from his bank account without him being a customer of the company. Complaints against the company by the data subject remained unsuccessful.

Fine: 75,000 euros

[Spain, Feb 2020] Iberdrola Clientes

Iberdola Clientes, an electricity company, **terminated the data subject's contract without its consent**, concluded three new contracts with the data subject, **processed his personal data unlawfully and transferred the plaintiff's personal data to a third party without legal basis**. In addition to this fine the AEPD also imposed another fine in the amount of EUR 50,000 under the old Spanish Data Protection Law.

Fine: 80,000 euros

EXAMPLES of cases involving Consent

[Spain, Dec 2020] Online Services involving children's data

- The Spanish DPA (AEPD) fined the operator of the online store banderacatalana.cat. for a violation of Art. 13 GDPR. The operator stated on its **website privacy notices that a minimum age of 13 or sufficient legal capacity was required to subscribe to the newsletter**. It was also stated that filling out the newsletter subscription form would be considered as consent to the processing of personal data. This constitutes a violation of the GDPR, as **according to Art. 8 GDPR, the processing of personal data of under-16-year-olds requires the consent of the holder of parental responsibility over the child**.
- **Fine**: 10,000 euros

Less than 10% of all cases involve *right to access*

Rights of Individuals	CY2018	CY2019	CY2020	Grand Total
15. Right to access	3	13	24	40
21. Right to object		7	12	19
17. Right to Erasure		5	11	16
18. Right to restrict processing	1	1	1	3
23. Restrictions			1	1
16. Right to correction			1	1
Number of enforcement cases	*29*	*163*	*319*	*511*

There were 16 cases across the EU involving Right to Erasure

Country	15. Right to access	21. Right to object	17. Right to Erasure	18. Right to restrict processing	23. Restrictions	16. Right to correction
BELGIUM	3	2	3			
BULGARIA	3					
CROATIA	1					
CYPRUS	2					
CZECH REPUBLIC	3					
DENMARK	1					
FINLAND	1					
FRANCE	1	3	1			
GERMANY	2	2	1			
GREECE	3	2				
HUNGARY	8		3	3		
ISLE OF MAN	1					
ITALY	5	3	3			1
LATVIA			1			
PORTUGAL	1					
ROMANIA	2	2	3			
SLOVAKIA	1					
SPAIN	1	5			1	
SWEDEN			1			
NETHERLANDS	1					
Grand Total	40	19	16	3	1	1

- Cases involving right to erasure is highest in Hungary, Italy and Romania.
- Only Hungary had cases involving right to restrict processing

EXAMPLES of cases involving Right-to-be-Forgotten

[Belgium, July 2020] Google Belgium

- A Belgian citizen had requested the removal of links containing negative information about him. The request was refused by Google.
- The Litigation Chamber of the Belgian DPA found that **some of those links were needed for public interest and should not be removed**: the citizen plays indeed a role in public life and the links concerned a presumed relation with a political party. The **other links contained information that was outdated, unsubstantiated and could seriously damage the reputation of the citizen.** The Belgian DPA considers that those links should have therefore been delisted by Google.
- **Fine**: 600,000 euros

EXAMPLES of cases involving Right-to-be-Forgotten

[Latvia, 2019] Online Services

- A merchant who provides services in an online store has infringed the 'right to be forgotten' pursuant to Art. 17 GDPR when he was **repeatedly requested by a data subject to delete all his personal data**, in particular his/her mobile phone number, which the merchant had **received as part of an order**. Nevertheless, the merchant repeatedly sent advertising messages by SMS to the data subjects mobile phone number.
- **Fine**: 7,000 euros

There were 20 cases involving Privacy by Design

Demonstrating Accountability	CY2018	CY2019	CY2020	Grand Total
25. Privacy by design		9	11	20
37. DPO		3	4	7
24. Responsibility of the controller		2	5	7
35. DPIA		1	4	5
36. DPIA Consultation		1	1	2
30. Records of processing activities			1	1
Number of enforcement cases	*29*	*163*	*319*	*511*

More cases of DPIA in 2020. There were also new cases involving DPIA consultation and records of processing

Cases involving demonstrating accountability on the rise

Country	25. Privacy by design	37. DPO	24. Responsibility of the controller	35. DPIA	36. DPIA Consultation	30. Records of processing activities
AUSTRIA		1				
BELGIUM	1	2	2			1
BULGARIA	4					
FINLAND				2		
GERMANY	1	2				
GREECE	2					
HUNGARY	4		3			
ITALY	3		2			
NORWAY				1		
POLAND	2					
ROMANIA	3					
SPAIN		2				
SWEDEN				2	2	
Grand Total	20	7	7	5	2	1

- 4 member states have cases involving **DPO**
- 3 member states have **enforced DPIA**. Sweden is the only member state to have case involving DPIA consultation
- Belgium had a case involving Records of Processing

EXAMPLES of cases involving Privacy by Design

[Romania, June 2019] UNICREDIT BANK S.A.

- The sanction was applied to UNICREDIT BANK S.A. as a result of the **failure to implement appropriate technical and organisational measures**, both within the determination of the processing means and processing operations themselves, **designed to effectively implement data protection principles, such as data minimisation**, and to integrate the necessary safeguards in the processing, in order to meet the GDPR requirements and to protect the rights of the data subjects.
- This led to the **disclosure of data concerning the personal identification number and the payer's address** (for situations where the payer performs the transaction from an account opened with another credit institution – external transactions and cash deposits) **and data concerning the payer's address** (for situations where the payer made the transaction from an account opened with UNICREDIT BANK SA – internal transactions) in the documents containing the details of transactions and made available online to payment customers, for a number of **337,042 data subjects**, during the period of the 25th of May 2018 – the 10th of December 2018.
- **Fine**: 130,000 euros

EXAMPLES of cases involving DPO

[Germany, 2019] Facebook Germany GmbH

- Whereas Facebook Ireland had appointed a data protection officer for all group companies located in the EU, **this appointment was not notified to the DPA Hamburg**, competent authority for Facebook Germany GmbH. The fine was calculated on the basis of the turnover of the German branch (EUR 35 million).
- **Fine**: 51,000 euros

EXAMPLES of cases involving DPO

[Belgium, 2020] Proximus SA

- According to the data protection authority, the company's data protection officer was not sufficiently involved in the processing of personal data breaches and **the company did not have a system in place to prevent a conflict of interest of the DPO**, who also held numerous other positions within the company (**head of compliance and audit department**), which led the DPA to the conclusion that the company's **DPO was not able to work independently**.
- **Fine**: 50,000 euros

EXAMPLES of cases involving DPIA/Consultation

[Finland, May 2020] Taksi Helsinki

- The Office of the Data Protection Ombudsman started an investigation on Taksi Helsinki's personal data processing in November 2019. Serious deficiencies were found in the company's processing of personal data.
- The company **had not assessed the risks and consequences of processing personal data before introducing a camera surveillance system** that records audio and video in its taxis and had also **failed to conduct data protection impact assessments of its processing activities, including the surveillance of security cameras, the processing of location data, automated decision making and profiling as part of its loyalty program.**
- **Fine**: 72,000 euros

EXAMPLES of cases involving DPIA/Consultation

[Norway, July 2020] Municipality of Rælingen

- Fined for the **processing of children's health data in connection with disability** through the digital learning platform 'Showbie'.
- The Municipality **had failed to carry out a Data Protection Impact Assessment ('DPIA')** in accordance with Article 35 of the GDPR prior to the start of the processing and **had not taken adequate technical and organisational measures** in accordance with Article 32 of the GDPR, resulting in an increased risk of unauthorised access to the personal data of the pupils.
- **Fine**: 46,660 euros

EXAMPLES of cases involving Records of Processing

[Belgium, Nov 2020] Social Housing Company

- The complainant argues that there is **camera surveillance in several residential units of the apartment**. According to the complainant, the **privacy policy does not mention anything about camera surveillance**. Complainant also wants to know the legal basis and purpose of this processing.
- In the renting agreement, cameras are mentioned but nothing more. The cameras were installed for safety, on request of some residents and are legally registered. The DPA determined that it wasn't clear why the cameras were installed exactly nor do the elements brought up suffice to determine if the cameras are compliant to the the law on cameras.
- **No register of camera processing was kept** (article 6 § 2 Camera law) **nor was the retention period of 30 days respected** (article 6 § 3 Camera law).
- The DPA found a violation of the requirement to keep a register of processing activities of Article 30 of GDPR and storage limitation.
- **Fine**: 1,500 euros

Other Articles	CY2018	CY2019	CY2020	Grand Total
Processor Responsibilities				
28. Processors with sufficient guarantees	1	2	5	8
Cooperation with the supervisor authority				
31. Cooperation with the supervisor		1	10	11
58. Powers - Insufficient cooperation with supervisory authority		3	19	22
Breach Notification				
33. Breach notification	1	8	13	22
34. Breach comm to data subject	1	2	5	8
Cross-borders Transfers				
48. Transfers or disclosures not authorised by Union law			1	1
Number of enforcement cases	*29*	*163*	*319*	*511*

- More cases in 2020 involving Processors, Failure to co-operate with supervisory authority, Breach notification.
- 2020 registered first case of breach of cross-border transfer

Country	28. Processors with sufficient guarantees	29. Processing under the authority of the controller or processor
FRANCE	1	
GERMANY	2	
ITALY	3	1
POLAND	1	
SPAIN	1	
Grand Total	8	1

EXAMPLES of cases involving Processors

[Italy, April 2019] Rousseau

- A number of websites affiliated to the **Italian political party Movimento 5 Stelle** are run by means of a **data processor, through the platform named Rousseau**.
- **The platform had suffered a data breach** during the summer 2017 that led the Italian data protection authority, the Garante (data protection authority), to require the implementation of a number of security measures, in addition to the obligation to update the privacy information notice in order to give additional transparency to the data processing activities performed.
- While the update of the privacy information notice was timely completed, the Garante, raised its concerns as to the **lack of implementation on the Rousseau platform of some of GDPR related security measures**. **Interestingly, the fine was not issued against the Movimento 5 Stelle that is the data controller of the platform, but against the Rousseau association that is the data processor.**
- **Fine**: 50,000 euros

EXAMPLES of cases involving Processors

[Italy, Sep 2020]

- According to the data protection authority, **personal information about participants in a public competition had been unlawfully disclosed online**. The reason for this was that, due to a configuration error, a list of the codes assigned to the candidates was temporarily accessible on the platform, which allowed access to the documents submitted by the candidates with their personal data.
- This was a **violation of the principle of protection of information security** for which Scanshare - which was the processor of the data on behalf of the controller 'Azienda Ospedaliera di Rilievo Nazionale 'Antonio Cardarelli'' (a private hospital).
- In addition, the data protection authority found that the information obligations were also not complied with and that the hospital had also **not provided a sufficient data processing agreement with the data processor** Scanshare
- **Fine**: data controller - 80,000 euros; data processor - 60,000 euros

Important for organisations to co-operate with supervisory authority

Country	58. Powers - Insufficient cooperation with supervisory authority	31. Cooperation with the supervisor
BELGIUM	1	2
BULGARIA		1
GERMANY		
GREECE	1	
POLAND	4	4
ROMANIA	8	2
SPAIN	8	2
Grand Total	22	11

EXAMPLES of cases involving Insufficient Co-operation with Regulators

- **[Poland, July 2020]** Office for Geodesy and Cartography - **Refusal of access to the premises** by the supervisory authority in the course of an audit.

  Fine: 22,300 euros

- **[Poland, July 2020]** After three subpoenas to East Power, in which the latter **failed to provide sufficient explanations on a direct marketing complaint**, the data protection authority found that East Power had **deliberately obstructed the course of the procedure** or at least failed to comply with its obligations to cooperate with the supervisory authority.

  Fine: 3,400 euros

- **[Spain, Nov 2020]** Xfera Móviles **had failed to cooperate with the AEPD in the investigation of privacy violations**. Xfera Móviles had neither responded to the request for information nor provided any required documentation.

  Fine: 20,000 euros

12 member states have enforced breach notification

Country	33. Breach notification	34. Breach comm to data subject
CYPRUS	1	
DENMARK	1	1
FRANCE	3	
GERMANY	2	2
HUNGARY	4	2
IRELAND	2	
ITALY	1	
LITHUANIA	1	
POLAND	2	2
ROMANIA	3	
SPAIN	1	
SWEDEN	1	1
Grand Total	22	8

EXAMPLES of cases involving Breach Notification

[Poland, Dec 2020] Towarzystwo Ubezpieczeń i Reasekuracji WARTA S.A.

- In May 2020, the DPA received a notification from a third party about a personal data breach involving an insurance agent acting as a processing agent for Towarzystwo Ubezpieczeń i Reasekuracji WARTA S.A. who **sent an insurance policy to an unauthorized addressee by email**.
- The document contained personal data concerning, among others, surnames, first names, residential addresses and information on the subject of the insurance policy. As a result, the supervisory authority asked the controller to clarify **whether, regarding the sending of the electronic correspondence to an unauthorized addressee, a risk analysis on the data security of natural persons had been carried out**, which is necessary to evaluate whether a data breach had occurred. Such a breach requires notification to the DPA and the individuals affected by the breach. In the letter, the supervisory authority advised the controller how to notify the breach and asked for explanations.
- **Despite the letter requesting explanations, the controller did not report the data breach nor did it inform the data subjects about the incident.** The DPA therefore initiated administrative proceedings. Only as a result of the initiation of the procedure did the controller report the personal data breach and inform two individuals affected by the breach.
- **Fine**: 18,930 euros

EXAMPLES of cases involving Breach Notification

[Poland, Dec 2020] TUiR Warta S.A.

- An insurance agent hired by the controller had **sent an email to unauthorized third parties** in regard to insurance policies that contained personal data of two of the company's customers **after they had mistakenly provided false email addresses**. The leaked data included data such as the names, email addresses and postal addresses of the data subjects.
- **The controller had not informed either the Polish DPA nor the data subjects about the data breach in a timely manner within 72 hours**. **The controller believed that there was no breach requiring notification because the data subjects themselves had mistakenly provided incorrect e-mail addresses.** The Polish DPA states that this circumstance does not release the controller from its obligation to report this data breach in a timely manner.
- **Fine**: 18,850 euros

EXAMPLES of cases involving Breach Notification

[Ireland, Dec 2020] Twitter International Company

- The Irish DPA (DPC) fined Twitter International Company for violating Art. 33 (1) GDPR and Art. 33 (5) GDPR for **failing to notify the DPA in a timely manner of a data breach and not adequately documenting that breach**.
- The data breach concerned the privacy settings of user posts on the social media platform Twitter. There, users have the option to set the visibility of their posts to private or public. Private posts can only be seen by subscribers of the respective user profile, while public posts are visible to the public. **A programming bug in Twitter's Android app resulted in some private posts being visible to the public.**
- The DPA found that Twitter had not properly fulfilled its reporting and documentation obligations. Twitter's legal team became aware of the error on January 2nd, 2019, and it was not until January 8th that the company informed the DPC. Consequently, **the company failed to inform the DPC within the 72-hour period required** by Art. 33 (1) GDPR. Furthermore, **it had failed to adequately document the incident** in accordance with Art. 33 (5) GDPR.
- **Fine**: 450,000 euros

Articles that have yet to be Enforced

PRINCIPLES

Art. 5	Principles relating to processing of personal data
Art. 5	5a Lawfulness
Art. 5	5b Purpose Limitatn
Art. 5	5c Data Minimizatn
Art. 5	5d Accuracy
Art. 5	5e Storage Limitation
Art. 5	5f Integrity & Confidentiality
Art. 6	Lawfulness of processing
Art. 7	Conditions for consent
Art. 8	Conditions applicable to child's consent in relation to information society services
Art. 9	Processing of special categories of personal data
Art. 10	Processing of personal data relating to criminal convictions and offences
Art. 11	Processing which does not require identification
Art. 12	Transparent information, communication and modalities for the exercise of the rights of the data subject

RIGHTS OF INDIVIDUALS

Art. 13	Information to be provided where personal data are collected from the data subject
Art. 14	Information to be provided where personal data have not been obtained from the data subject
Art. 15	Right of access by the data subject
Art. 16	Right to rectification
Art. 17	Right to erasure (Right to be forgotten)
Art. 18	Right to restriction of processing
Art. 19	Notification obligation regarding rectification or erasure of personal data or restriction of processing
Art. 20	Right to data portability
Art. 21	Right to object
Art. 22	Automated individual decision-making, including profiling
Art. 23	Restrictions

CONTROLLERS & PROCESSORS

Art. 24	Responsibility of the controller
Art. 25	Data protection by design and by default
Art. 26	Joint controllers
Art. 27	Representatives of controllers or processors not established in the Union
Art. 28	Processor
Art. 29	Processing under the authority of the controller or processor
Art. 30	Records of processing activities
Art. 31	Cooperation with the supervisory authority
Art. 32	Security of processing
Art. 33	Notification of a personal data breach to the supervisory authority
Art. 34	Communication of a personal data breach to the data subject
Art. 35	Data protection impact assessment
Art. 36	Prior consultation
Art. 37	Designation of the data protection officer

Executive Summary

- While **number of enforcements in the EU has doubled from 2019 to 2020** despite COVID19, **number of cases at the member state level (country) is still miniscule.**
- **Luxembourg and Slovenia are** the only EU member states **yet to have enforced the GDPR**.
- Interesting to see 2 countries/states – **Norway and Iceland** in the European Economic Area **have enforced the GDPR**
- **Google still holds the record fine of 150m in total EUR**. However, **9 other companies** have been fined **more than 10m EUR in 2020**
- **15 companies were fined more than 1m EUR** in 2020 (vs 5 in 2019) – makes up >93% of overall fines
- **Top 3 areas in GDPR enforcements** - GDPR principles (65% of all cases), lawful basis (41%), as well as Security of processing and Transparency (both 23%)

Implications for ASEAN

- Importance of **GDPR as a de facto reference standard**

- GDRP Enforcements are **operational nature vs legal** - cases can also happen in ASEAN

- **Key areas** to focus on
  1) Comply with **data protection principles**
  2) Ensure **lawful/legal basis** for processing (including stricter consent requirements)
  3**) Transparency** and **security of processing**

- **Do due diligence on third party processors** to ensure secure processing of personal data

- Importance of **demonstrating accountability** (including co-operation in investigations) to regulators (DPO, DPIA, DP by Design, Data Breach Notification)

Recommendations

- Implement a data protection management programme (DPMP) to sustain compliance efforts
- Address common risks / breach scenarios; importance of conducting data inventory / mapping to identify risks as first stage
  - Compliance risks
  - Personal data risks
  - Process risks
  - Product/Project Risks
- It's not just about putting policies in place – standard operating procedures and clear processes are KEY. Employees should understand them too.
- Go for Data Protection Trustmark Certification Achievement
- **Attend the IAPP CIPP/E which covers European Data Protection Laws**
- Go to www.dpexcentre.org (for more courses)

CIPP/E encompasses pan-European and national data protection laws, key privacy terminology and practical concepts concerning the protection of personal data and trans-border data flows.
https://www.dpexnetwork.org/courses/certified-information-privacy-professional-europe-sg/

NEXT RUN: 10 Mar 2021 – 12 Mar 2021

Developed by the International Association of Privacy Professionals (IAPP) and brought to Singapore by Straits Interactive, CIPM is the world's first and only certification in personal data protection programme management.
https://www.dpexnetwork.org/courses/certified-information-privacy-manager-sg/

NEXT RUN: 24 Mar 2021 – 26 Mar 2021

Certified Information Privacy Professional/Asia (CIPP/A)

CIPP/A is the first publicly available privacy certification that covers multiple jurisdictions in the Asia region. It addresses the data protection laws in Hong Kong, India and Singapore and the regional privacy concerns in this rapidly growing landscape.
https://www.dpexnetwork.org/courses/certified-information-privacy-professional-asia-sg/

NEXT RUN: 9 Jun 2021 – 11 Jun 2021

CIPT teaches technology and data professionals how to understand and integrate strategies and techniques to minimize privacy threats.
https://www.dpexnetwork.org/courses/certified-information-privacy-technologist-sg/

NEXT RUN: 29 Mar 2021 – 31 Mar 2021

THE END