CONFERENCE NOTES

Supported by

Contents

Welcome to the *GDPR - Three Years On* conference

Here we are again having our GDPR conference online despite the fact that we were convinced this year will be face to face. However, COVID-19 or not cases keep being decided and it is always important to stay up to date. Another year of learning and we have no doubt that the more years that pass by the more we shall keep learning.

Discussing cases as well as having speakers who are experts in the field is the best way to stay abreast with current developments and this is why we truly believe this conference is so valuable. Thank you for being part of it and a special thanks to those of you who have been attending from the very first time we organised this.

A big thank you goes to my business partner at Advisory 21, Mr Angelito Sciberras, my colleague at 21 Law, Dr Patrick Farrugia who helped extensively with the legal research, and our valuable speakers.

Hope that you will enjoy our conference and hope that we shall see you next year (who knows it may be face to face!)

Roselyn

Programme

09:15 - 09:30 **Registration**

09.30 - 09.45 **Three years in review** - *Dr David Ciliberti, Legal and Policy officer at DG JUST, European Commission*

09.45 - 10.30 **Case Law review (Local & Foreign)** - *Dr Roselyn Borg, 21 Law & Dr Sarah Cannataci, Fenech & Fenech Advocates*

10.30 - 10.40 **Break**

10.40 - 10.55 **GDPR Post Pandemic, an overhaul? –** *Mr Axel Voss, Member of the European Parliament*

10:55 - 11:45 **Case Law review (Foreign)** - *Dr Roselyn Borg, 21 Law & Dr Sarah Cannataci, Fenech & Fenech Advocates*

11.45 - 12.30 **The Questions you always wanted to ask the IDPC** - *Mr Angelito Sciberras, Advisory 21 asks Mr. Ian Deputy Commissioner, Office of the Information and Data Protection Commissioner. Participants can also ask their questions to the IDPC and the other speakers.*

12:00 **End of Conference**

The Speakers

Dr Roselyn Borg

Dr Borg is a dual qualified lawyer specialising in employment law. She has over 17 years' experience working locally and overseas. She has developed and delivered training programmes and has advised several employers on various employment law and data protection issues.

She also represents clients at the Employment Tribunal. She graduated at the University of Malta and then pursued her studies in the UK, where in 2009 she also set up a boutique employment law practice Borg Knight Employment Solicitors which she still runs. In 2012 she moved back to Malta and set up 21 Law, also a practice specialising in employment law.

Roselyn has created and delivered several courses including workshops and courses on data protection. She is a visiting lecturer at the University of Malta. She also contributed to a number of publications and also the co-author of the book GDPR for HR Professionals.

Roselyn is one of the founding partners of 21 Academy where she is also the Head of Institution.

Dr Sarah Cannataci

Sarah is an Associate at Fenech & Fenech Advocates working with the firm's Technology, Media and Telecoms Law (TMT) department. She started practicing in data protection, privacy, and intellectual property in 2014 and joined the International Practice department at Fenech & Fenech Advocates in 2017.

Sarah obtained a Bachelor of Laws (Honours) from the University of Malta in 2016, basing her Research Paper on the erosion of privacy by search engines and the Right to be Forgotten as envisaged within the General Data Protection Regulation. She qualified as a lawyer with a Masters in Advocacy in 2017 and was called to the Maltese bar in 2018.

As part of the Fenech and Fenech team, Sarah has advised and assisted clients in relation to data protection, information technology, cybercrime, gaming law as well as telecommunications. Furthermore, Sarah also assists clients in trademarks, copyright, and design rights amongst other intellectual property issues.

Dr David Ciliberti

David Ciliberti is a Legal and Policy officer at DG JUST, European Commission. As part of his tasks, he has reviewed national laws implementing the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) and has represented the European Commission before the European Data Protection Board (EDPB), in particular in the financial matters sub-group. He is currently working on the legal revision of the Consumer Credit Directive.

Prior to joining the European Commission, Dr Ciliberti served as a Justice and Home Affairs Attaché at the Maltese Representation to the EU. He represented Malta during the negotiations of the GDPR and LED. During the Maltese Presidency of the Council of Ministers, Dr Ciliberti chaired the Working Party on Information Exchange and Data Protection (DAPIX). Under his helm, Council adopted a General Approach paving the way to the adoption of Regulation 2018/1725.

Earlier in his career, Dr Ciliberti worked at the European Court of Justice (CJEU). He holds a Master degree from the College of Europe, Bruges, and regularly lectures at different European universities.

Mr Ian Deguara

Ian was appointed as Information and Data Protection Commissioner with effect from 21st December 2020.

He was one of the first employees to join the Office of the Information and Data Protection Commissioner in December 2002 after successfully completing his studies at the University of Malta, where he obtained a degree in computing and also in management.

Initially, even before the Data Protection Act came into force in July 2003, his role included assisting the Commissioner to smoothly implement the novel set of rules which introduced fundamental rights to data subjects and imposed obligations on data controllers. Mr Deguara was involved in the investigation of data protection and freedom of information complaints, advised the Commissioner on local and European data protection issues and other technological matters, and represented the Office in expert groups of the European Data Protection Board.

Mr Deguara formed part of the national taskforce set up with the mandate to prepare the necessary legal instruments to implement the General Data Protection Regulation. He delivered various information sessions and participated as an expert speaker in a number of conferences which were organised to raise awareness on the reformed data protection package.

Mr Angelito Sciberras

Angelito has worked in the Health Care, Journalism, Marketing, Sports and Administration fields. He has vast experience in Human Resources, Customer Care and Event Management. Angelito has developed and delivered training programmes in the IT field and in Data Protection particularly on the GDPR and delivered them at educational institutions as well as in house at various clients.

He is also a partner at Advisory 21, 21 Academy and runs 21 Business Centre. Angelito co-authored the book GDPR for HR Professionals which was published in May 2018. He acts as an external data protection officer with different organisations.

He has a post graduate diploma in Business Management and is currently widening his horizons by studying Liberal Arts and Sciences at the University of Malta and a Masters in Business Administration at the University of Suffolk.

Mr Axel Voss

Twenty-two years senior management experience in the ICT industry, currently Chief Executive Officer at CyberSift, a Cyber-Security solutions provider.

Previous to this role Brian was the Chief Technology Officer at 6PM Plc. Responsible for the overall and long-term technology vision and strategy of the company in the various sectors it operates. Driving innovation from the research and development perspective he worked closely with different teams in the company in bringing products to market that offer immediate business value to the company's customers.

Brian had an active role in working with the company's leading customers in Healthcare, Pharmaceutical Manufacturing and igaming industries where he was involved in bespoke and product application development as well as product strategy.

Prior to transitioning to the CTO role at 6PM, Brian was the co-founder of a systems integration firm where he held the position of Director of Technology for fifteen years. He also recently co-founded Senseon Solutions a firm specialized in ICT Security offering penetrating testing, PCI-DSS consultancy and ICT audit services to both local and international firms.

Brian holds a B.Pharm (Hons.) degree from the University of Malta, is a CISA certified Information Systems Auditor as well as a PRINCE2 Project Manager.

The 5 highest fines imposed by Supervisory Authorities so far

2018 was a monumental year for data privacy law. The introduction of the General Data Protection Regulation (GDPR) saw an upheaval in data processing systems of practically all data European entities and organisations, in an effort to get in line with the new Regulation which was to come into force in May of the same year. Whilst the benevolent intent in protecting data subjects' personal information is commendable, one cannot but point out that the incredibly aggressive fines which could be handed out in the case of a violation had a greater force in terms of urging us all to get in line with the law.

Over the two years during which the Regulation has been in force across all European Union member states, certain fines handed out by individual states' national supervisory authorities have been jaw-dropping. Lat year we reported that the highest fines till then were those imposed by the UK's Information Commissioner's Office (ICO) in July 2019 to British Airways for €204,600,000 and Marriot International for €110,300,000. Upon appeal both fines were reduced. The first to €22,406,000 and the second to €20,450,00 which places them in the fourth and fifth rank. Thus, the French authority (CNIL) penalty of **€50 million** handed out by to Google in 2019 is now the highest. The fine was imposed as the CNIL concluded that Google failed to provide sufficient and clear information to users about its data processing.

The second highest fine was imposed on the Swedish Retail Company H&M which has been subjected to a **€35 million** fine by Hamburg's Data Protection Authority. Since 2014, the company had been illegally and excessively monitoring Nuremberg employees' private lives. The company held employees' data related to inter alia the employee's vacations, illnesses and diagnoses, family issues and religious beliefs. This data was collected and stored without the knowledge of the data subjects and without any proper basis for processing such data. Moreover, this data was accessible by many company managers. All this was exposed in late 2019 due to a configuration error, which made the data accessible to everyone within the company for a few hours.

The Italian supervisory authority's **€27.8 million** fine to **TIM** for data violations tanks in the third place. Tim was found to have insufficient legal basis for data processing. The Italian Supervisory Authority (Garante) had been receiving a distressing number of complaints from

TIM service subscribers who were being consistently bombarded by promotional calls to which they had not consented, whilst others had specifically opted-out from being contacted for marketing purposes. The Italian Garante noted several other unfair practices in the service provider's subscription policies, many of which were filled in using paper format and contained one single opt-in check box, which contained numerous conditions including promotions. Furthermore, a specific phone scheme incentive was available to consumers only on condition that one consents to direct marketing upon subscribing to it.

As announced during last year's GDPR conference, the office of the Information and Data Protection Commissioner started publishing the local legally binding decisions. While the highest fines in Malta were imposed for an ill addressed Subject Access Request (€20,000) and the unsolicited sending of direct marketing communications (€15,000), most of the local cases were investigated following a complaint while only 37% of the cases were as a result of a personal data breach. 29% of the investigated controllers were landed with a fine while only one case ended up with no corrective action against the controller. In most of the other cases the controllers were reprimanded.

Most of the case in Malta dealt with disclosure of data to the wrong data subjects, followed by CCTV cameras issues. In the first case most of the errors seem to have been caused through emails, while in the CCTV revolved around the capturing of public access areas and, or spaces.

We have also listed the highest known fine imposed in each country so far[1].

Country	Fine	Entity	Type of Breach
France	€50,000,000	Google Inc.	Insufficient legal basis for data processing
Germany	€35,258,708	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Non-compliance with general data processing principles
Italy	€27,800,000	TIM	Insufficient legal basis for data processing
United Kingdom	€22,046,000	British Airways	Insufficient technical and organisational measures to ensure information security
Austria	€18,000,000	Company in Medical Sector	Insufficient fulfilment of information obligations
Spain	€8,150,000	Vodafone España, S.A.U.	Insufficient fulfilment of data subjects rights
Sweden	€5,000,000	Google LLC	Insufficient fulfilment of data subjects rights
Norway	€5,000,000	Google LLC	Insufficient fulfilment of data subjects rights
Bulgaria	€2,600,000	National Revenue Agency	Insufficient technical and organisational measures to ensure information security
The Netherlands	€900,000	UWV (Dutch employee insurance service provider)	Insufficient technical and organisational measures to ensure information security
Poland	€660,000	Morele.net	Insufficient technical and organisational measures to ensure information security
Belgum	€600,000	Google Belgium SA	Insufficient fulfilment of data subjects rights
Ireland	€450,000	Twitter International Company	Insufficient fulfilment of data breach notification obligations
Portugal	€400,000	Public Hospital	Insufficient technical and organisational measures to ensure information security
Hungary	€288,000	Digi Távközlési Szolgáltató Kft.	Insufficient technical and organisational measures to ensure information security
Greece	€200,000	Telecommunication Service Provider	Non-compliance with general data processing principles
Denamrk	€160,000	Taxa 4x35	Non-compliance with general data processing principles
Latvia	€150,000	Unknown	Insufficient legal basis for data processing
Romania	€150,000	Raiffeisen Bank SA	Insufficient technical and organisational measures to ensure information security
Czech Republic	€118,500	Unknown	Insufficient legal basis for data processing
Finland	€100,000	Posti Group Oyj	Insufficient fulfilment of data subjects rights
Estonia	€100,000	Azeta.ee e-apteek	Insufficient legal basis for data processing
Cyprus	€70,000	LGS Handling Ltd, Louis Travel Ltd, and Louis Aviation Ltd	Insufficient legal basis for data processing
Lithuania	€61,500	Payment service provider UAB MisterTango	Insufficient fulfilment of data breach notification obligations
Slovakia	€50,000	Social Insurance Agency	Insufficient technical and organisational measures to ensure information security
Iceland	€23,100	InfoMentor ehf	Insufficient technical and organisational measures to ensure information security
Malta	€20,000	Unknown	Insufficient fulfilment of data subjects rights

[1] Source: GDPR Enforcement Tracker

Schrems II

The Schrems II case has garnered a reputation of being one of the greatest landmark cases of significance handed down by the Court of Justice of the European Union (CJEU). Essentially, the decision effectively invalidated the EU-US Privacy Shield data flow agreement.

The case was initiated in Ireland against Facebook in an attempt to invalidate the standard contractual clauses used for the purposes of transferring personal data form the EU to the US. Its main argument was based on the premise that data which finds itself in the United States could easily be processed by US intelligence agencies without the need to inform the data subjects. The claimant argued that this transfer therefore did not provide adequate safeguards for the protection of the data in question.

In fact, the CJEU concluded that US law's level of protection was not "equivalent to that guaranteed within the EU by the GDPR, read in the light of the Charter [of Fundamental Rights]". This was so because US law dictates that the interests of national security, public interest and law enforcement supersedes individual data subjects rights' to data privacy. Furthermore, decisions by the Ombudsman responsible for the Privacy Shield had no authority to bind the US government and authorities by its decisions, which also cast doubt on the safety of the Privacy Shield.

Chimp's Out

March 2021

A recent decision handed down by the Bavarian data protection authority considered a fashion magazine's use of Mailchimp, which is a US based email and newsletter marketing platform, ran strictly contrary to the reasoning of the CJEU in the Schrems II case.

The authority's investigation was triggered by virtue of a complaint made by a data subject, claiming the illegality of the fashion magazine's transfer of personal data to the US based platform.

The authority determined that the magazine rested upon the Standard Contractual Clauses to justify the transfer of personal data to the US for marketing (newsletter) purposes. However, this was insufficient as there was no guarantee that the data could not be compromised by US intelligence agencies. In fact, the Schrems judgment considered that whilst the Standard

Contractual Clauses were not effectively invalid by virtue of such decision, additional protective measures should have nonetheless been taken. This was not the case in this situation.

In this instance, no fine was imposed considering the company's understanding of and compliance with the authority's opinion and recommendations, together with the relatively minimal categories of personal data transmitted to the US based operator.was obtained. Whilst these principles have been largely developed in the criminal sphere, the decision at hand quotes a staggering amount of judgments which discuss these rules' applicability in the civil sphere. This is even the stance taken by the European Court of Human Rights (ECtHR), which concludes that illicitly obtained evidence does not necessarily render proceedings unjust.

Population Control

April 2021

A suspension order on the transfer of personal data submitted by virtue of the 2021 Portuguese Census was issued by the Portuguese data protection authority (CNPD) in light of the fact that such data was being transferred to an operator in the US.

Cloudfare Inc, based in California, was engaged by the Portuguese statistics authority to operate its census questionnaire. Whilst a formal data processing agreement was in place at the time, it did not provide for the adequate safeguards made necessary by virtue of the reasoning of the Schrems judgment. Urgent action became necessary in this case as by the time the CNPD got involved, the census questionnaire had already collected several categories of data of over 6,500,000 persons in Portugal.

CNPD
Comissão Nacional de Proteção de Dados

The Portuguese authority held that the possibility that US intelligence services could access the data within their own jurisdiction without the need to inform the data subjects concerned was a disproportionate interference with one's basic privacy rights in light of the rationale of the GDPR.

A Strong Defence

April 2021

In the wake of the Schrems conundrum, a French court was tasked with evaluating the legality of e-health service company Doctolib's transfer of data by its processor AWS Sarl, which is a subsidiary of Amazon Web Services and is based in the US. AWS Sarl was acting as a host repository for the personal data processed on Doctolib.

The French health authorities had been making use of the platform to organise and issue COVID-19 vaccination appointment schedules. In this case, the French court provided an interesting outlook into the platform's safeguards for EU citizens and how they applied in terms of the teachings handed down in the Schrems decision.

The court initially noted how the agreements between Doctolib and AWS Sarl covered a specific procedure to be followed in case an access request is submitted at any point, particularly where such request is made by a governmental body or authority (the drafting thereof would therefore cover access requests by US intelligence agencies). The court considered this to be a very effective safeguard measure against unrestricted data access by US authorities.

Further protection was provided to data subjects' rights as the data being transferred was encrypted, with the key held by a third party located in France. This provided an additional layer of safety to the data in question, together with the fact that the data in question only related to contact details and not to any sensitive medical data relating to one's eligibility (or otherwise) for vaccination. Furthermore, the data was in line with storage limitation principles as retention of this data was set for a very limited period.

CCTV

With Suspicious Eyes

December 2020

The Lower Saxony (Germany) Data Protection Commissioner has fined electronics store notebooksbilliger.de €10,400,000 for excessive CCTV coverage within several areas of the workplace, even including staff rooms. This is the highest penalty imposed by the Lower Saxony Commissioner, and the second highest in Germany.

During the investigation, the company revealed that the point behind the installation of the cameras was to track the movement of goods around the warehouses and shop floors and to deter and prevent theft. The Commissioner inquired as to whether the company had any specific suspicion of any thefts being committed, however no such suspicion subsisted but the installation of CCTV was merely a preventive measure. In fact, such surveillance is only permissible for a specified period of time in case of a specific suspicion by the employer, harking back to the reasoning expounded in the Lopez Ribalda case.

The fine was imposed as the camera surveillance had been in place for over two years without any legal justification, as a general suspicion does not suffice. There are other less intrusive measures which could be made use of in case of suspicion of theft. The Commissioner explained that video surveillance is "a particularly invasive encroachment on a person's rights", and subsequently also pointed out that the surveillance also affected clients' rights, most especially since due to the nature of the stores (electronics) clients spend quite some time trying products out, so much so that seating areas are also available.

Office with a View

March 2021

A company was fined €14,900 by the Norwegian Datatilsynet for violations of privacy rights due to excessive CCTV coverage through a webcam installed at the top of its office building.

The footage captured a wide angle around a public street, which included several establishments such as a parking area, several shops and other buildings, and also the town hall. The footage was furthermore broadcasted on YouTube and a viewer could rewind up to 12 hours of footage.

Whilst the camera could not specifically identify data subjects' faces, it was amply clear that individuals' personal traits, such as hair colour, clothes and other specific characteristics, could be identified. This therefore not only served a purpose for the company to be able to track its employees when out in public within the vicinity of its office building but could also be used by any other person watching the broadcast on YouTube to track other data subjects who happened to be in the street. The Datatilsynet highlighted that employees (and other persons out in public) could not reasonably expect to have their movement tracked when they are outside the office buying food or other personal items from the stores around the building. The severity of this breach was further heightened by the fact that the coverage was broadcast on the internet.

The Customer is Always Right

September 2020

An issue arose within a Deichmann store in Kaposvar, Hungary, wherein a client who had already left the store realised that he had paid with a larger bill than he had initially thought. He later went back into the store to claim the correct change, but the salesperson refused. The client later sent a letter of complaint the company highlighting his concerns and requested that he is allowed to view the CCTV footage wherein he is seen at the cash counter.

The client's request was rejected on the basis that the CCTV footage can only be viewed against a police report having been filed. Once the report had been filed, Deichmann informed the data subject that the footage had already been deleted.

Upon investigation, the NAIH found that Deichmann operated a multitude of surveillance cameras within its stores and that there were several other breaches regarding requests of a similar nature.

A fine of €54,800 was imposed on the company for failing to adhere to the data subject's request for access and for retention of the footage once a specific request had been lodged, thus lacking the appropriate technical and organisational measures to safeguard data subjects' rights in this light.

We can't all be James Cameron

Whilst no fines have been issued by the Maltese IDPC throughout the last year in relation to CCTV camera privacy breaches, the authority has issued numerous reprimands. These generally covered CCTV systems which were installed without the proper signage on display, or more commonly where public spaces were being recorded.

It is becoming increasingly common to find persons who affix cameras to their property as part of home security systems, and the manner and angle in which these are installed is crucial so as to avoid the capturing of public areas.

Data Breaches

Art. 4 GDPR – 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Booking Error

March 2021

In 2018, a cyberattack on several hotels in the United Arab Emirates resulted in several Booking.com login details being hacked, therefore allowing the hackers to gain access to the personal Booking.com profiles of over 4,000 customers who had booked stays at the affected hotels.

The danger posed was amplified in light of the fact that the profiles contained several credit card details, which also included the CCV code in some cases. It also came to light that the hackers attempted to contact the clients directly, impersonating Booking.com agents, in an attempt to gather further data relating to credit cards.

The Dutch authorities imposed a fine of €475,000 on Booking.com but specified that the amount was in no way related to the company's security arrangements (or lack thereof). Rather, the fine of close to half a million Euro was strictly related to the company's failure to notify the authorities in time – 22 days late in fact. The GDPR imposes a 72-hour window as a maximum period for reporting breaches. This was amplified even further considering the sensitivity of the data being breached, and the authority furthermore noted that the danger would have even existed even if regular data was stolen, such as names and contact details, as phishing scams could be easily attempted with this kind of data at hand.

Flight Risk

March 2021

Airline company Air Europa was hit with a €600,000 fine issued by the Spanish AEPD following a malware hack to their systems which managed to access the data of almost half a million clients, with a totality of around 1.5 million records.

Several bank card details (including card numbers, expiry dates and CVVs) were breached, and around 4,000 cards were actually used for fraudulent transactions. Several shortcomings from Air Europa's side in this regard were highlighted by the AEPD, such as lacking technical security systems by default and by design, specifically with relation to the fact that no multi-factor authentication security existed, which was to be expected considering the highly confidential nature of the data contained in the system.

The severity of the case was further exacerbated by the fact that the airline classed the breach as 'medium risk' and decided against informing the affected data subjects, stating that it would be impossible to identify them all. A public notification was also decided against as the breach was not considered to be so severe as to make it necessary. Furthermore, the AEPD was only informed of the breach over a month after the company became aware of the incident. In fact, €100,000 from the total fine was specifically imposed as a sanction against the tardiness in notifying the authority.

More Viruses?

The IDPC has issued decisions on several cases relating to serious data breaches, whether through hacking of systems, unauthorised access by third parties, or otherwise through negligence. Penalties ranged significantly from mere reprimands to fines reaching as high as €5,000.

Employment

Nosy, Nosy

October 2020

A ground-breaking fine was imposed by the Hamburg Commissioner (HmbBfDI) wherein H&M was slapped with a €35,300,000 fine for violating its employees' data privacy rights, with this fine being the highest one given in Germany since the GDPR came into force in 2018, and the second highest across the EU.

The company's service centre in Nuremberg had been collecting swathes of personal data regarding its employees' private lives, consisting of notes on illness absences and symptoms, return-to-work interviews, specific details about vacations, and also several other details including for instance religious belief, which were obtained during casual conversations with superiors. This constituted a significant unnecessary interference within employees' private lives, and the severity of this issue was further heightened by the fact that it was also discovered that this data was also put to use in the making of decisions relating to the employee's tenure with the company.

At one point, these records became accessible on the company's internal system due to a configuration error. Following investigations by the authorities, the company issued an apology to all its employees and also proposed to pay damages to the affected employees, whilst guaranteeing the implementation of several data protection mechanisms. These actions were taken into consideration in calculating the fine to be imposed.

It's Getting Awkward

November 2020

In an effort to ensure confidentiality of client data, a call-centre issued a clean desk policy wherein employees were prohibited from keeping certain items (such as handbags, phones or other devices) on their desks. An exception was made with regard to any medicine boxes and sanitary pads. However, the excepted goods were to be kept strictly in clear sight on the employee's desk and were not to be hidden beside or under other items.

Following complaints, a subsequent policy was issued after a few months which permitted that medicines and sanitary pads can in fact be kept in a small case. However, the policy dictated that if such case would be larger than a smartphone in size, the employee would have to inform HR of the types of medicines intended to be kept in the case.

The Italian Garante noted that whilst the employer may process certain particulars of the employee for the purpose of enforcing the employment contract (relationship), when it comes to special category data (which covers data related to the employees' health) the employer must have a specific legitimate ground to process it. In conclusion, the Garante imposed a fine of €20,000 on the company for processing special category data of employees unnecessarily and in a disproportionate manner.

Data Disposal

Recycle Wisely

October 2020

A private individual brought to the attention of the Irish health authorities the fact that a collection of physical (printed) data of patients of the Cork University Maternity Hospital had been found in a recycling disposal facility outside of the city, wherein the authority reported the issue to the Irish Data Protection Commission.

The authority considered this to be a breach of data subjects' rights, considering that the collection of documents covered around 80 patients, out of whom 6 had special category data relating to their medical history included.

The Commission noted that this was a breach of the Hospital's obligation to implement "appropriate technical and organisational measures" to ensure the security of patient data, especially considering the sensitive nature thereof. Therefore, it issued a fine of €65,000, whilst also ordering the health authorities to ensure that all patient information systems is ensured to be fully compliant with the standards enunciated in the GDPR.

Ospideal Maithreachais
na h Ollscoile Corcaigh
Cork University
Maternity Hospital

Emails

Trust Issues

January 2021

The Polish Office for Personal Data Protection (UODO) received a report of a potential breach regarding an email attachment which contained confidential personal details. This email was mistakenly sent to the incorrect recipient.

The UODO attempted to make contact with the data controller, to point out the breach and explain the method to assess the severity and impact of the breach, and how to implement measures to ensure it is prevented in the future. The company replied, explaining that the breach had not been reported to the authority since the data which was erroneously sent was not considered sensitive. Furthermore, it argued that the mistaken recipient was known to the company and had confirmed that the data had been permanently deleted.

The UODO concluded that the declaration made by the incorrect recipient was insufficient and does not eliminate the risk of the breach, and that therefore a breach to the authority should have been submitted, nonetheless. The company was therefore fined €30,000 for the nature of the breach and its duration, intentional nature of the failure to report, and the lack of cooperation with the UODO.

Auto-Forward, Auto-Fine

May 2021

A company was placed under investigation by the Norwegian Datatilsynet following a report about its email auto-forwarding system, which activated itself immediately once an employee would be on sick leave. In this case, the employer was issued with a hefty fine of €40,000 for several violations relating to this system.

In one case of a particular employee's absence, the auto-forwarding remained active on the employee's inbox for well over a month following her return to work. The Datatilsynet investigated and concluded that the automatic auto-forwarding was a strict violation of the GDPR, considering the fact that the employees had never been made aware of this system. In addition to the fine, the authority ordered the employer to review its written procedures regarding employee email and inbox access.

The authority considered that emails have long been classified as personal data, even when these relate to a work email address. The employer may only access an employee's inbox in a limited number of cases.

Exposed

During the past year, the local scene was rocked by several reports of unauthorised disclosure of personal email addresses via emails sent to several recipients using the 'to' field rather than the 'bcc' field to input all recipient email addresses. In fact, fines of €2,500 each were meted out by the IDPC in two such local cases. A reprimand issued by the IDPC in 2020 also related to an organisation transmitting personal data relating to a data subject and his children in an email were unintended recipients were also copied in.

Marketing

The action or business of promoting and selling products or services, including market research and advertising.

Gone with the Wind

July 2020

In the latest spate in the Italian Garante's fines imposed for excessive marketing we find a €16,700,000 fine imposed on Wind in July 2020.

This classic data privacy breach through excessive telemarketing followed continued infringements following several prohibitory injunctions having already been imposed on the company under the pre-GDPR regime.

The breaches were several – disgruntled data subjects complained of direct marketing occurring through text messages, emails and phone calls. Inaccurate and incomplete privacy notices created stumbling blocks for data subjects to withdraw their consent to marketing or to be included in public marketing registers, and where it was possible, the withdrawal would only occur following 24 hours. At the same time, certain telephony apps operated by the same companies constrained data subjects to consent to marketing communications for use of the same.

Call Me Back

April 2021

The Italian authority was called upon to investigate a company following hundreds of complaints against excessive electronic marketing.

In this case, the authority noted the danger of abuse from various third-party marketing companies which organisations appoint to take care of their marketing activities. Such agencies commonly have no regard to data privacy legislation, and the Garante highlighted the fact that in this case, client consent to transfer of data to third-party marketing agents was never obtained, and this was quite serious since the centres in question are located outside of the European Union.

In this case, several complainants claimed that they were also receiving unsolicited WhatsApp messages requesting contact and identity details for the purposes of phishing and other fraudulent activities. The marketers' contact details were often fictitious and non-traceable.

The company was also found to be making use of call-me-back functions in an attempt to obtain implicit consent to marketing. Using such a system would mean that a recipient would receive a text to call back the sender's number (generally intended to be used when one is out of phone credit).

The company, Fastweb, was therefore fined €4,500,000 for processing huge volumes of personal data without data subject consent.

They Never Listen

March 2021

Following investigations initiated by almost 200 complaints submitted to the Spanish AEPD, Vodafone España was fined €8,000,000 for repeated data privacy breaches related to marketing. This has been the AEPD's highest issued fine to date.

Complainants noted that they had been at the receiving end of a deluge of marketing calls, texts and emails on behalf of the company. The data subjects had not consented to marketing and many of them were also not listed on the Robinson list (this list collects data of persons who wish to exclude themselves from marketing communications, also referred to as mail preference services).

The Spanish AEPD further took note of the fact that Vodafone España was in breach of its data transfer obligations, since not only was client data being transferred to third parties without consent, but it was also being transferred to marketing agents outside the EU (in this case, to Peru).

In assessing the facts and considering the fine to be issued, the authority also took into consideration the fact that the company had received numerous fines since 2018 and still had not regulated its position.

Breaches Galore

November 2020

Vodafone Italia became the subject of investigations by the Italian Garante, which considered the fact that this was not the first incident relating to data privacy right complaints due to excessive marketing in relation to this company, resulting in a fine of €12,250,000.

The Garante took note of several violations on the company platform, one of the most grievous being the use of fake telephone numbers emanating from unauthorised call centres which were not registered with the Italian Registry of Communication Operators for marketing purposes. Several such numbers were being used to send WhatsApp messages directly to data subjects without their consent, purporting to be acting on behalf of Vodafone Italia, and the Garante concluded that the likelihood of such communications were for spam, phishing and other fraudulent activities. The company was also found to be in breach of its consent requirements under the GDPR, for obtaining contact lists from external parties without the data subjects' consent.

The Italian authority concluded that the company was in significant breach of its consent obligations and also of its accountability and data protection by design requirements in terms

of its processing of personal data without a legitimate basis for aggressive marketing purposes.

No Junk Mail

'No junk mail' signs are an increasingly common sight on several household mailboxes, considering the colossal volume of promotional adverts, magazines and notices which make the rounds each day in Malta. If only it was that easy to have such a notice stuck onto our phones and email inboxes.

Reports on unsolicited marketing are in fact becoming quite common in Malta, and the IDPC is taking action on them. In fact, one of the highest fines issued to date relate to unsolicited marketing by data processors, with objection requests largely ignored. In fact, one such fine amounted to €15,000.

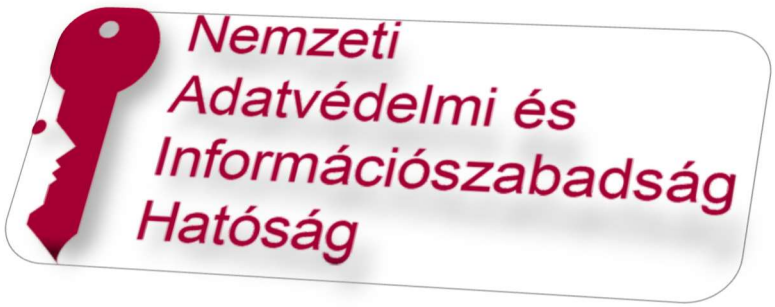
Special Category of Data

Art. 9 GDPR - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

Breach Pandemic

April 2021

The COVID-19 pandemic has seen a wave of data being processed in astounding volumes, whether for purposes of contact tracing, quarantining, and most recently vaccination. When processing personal data relating to health, one must always keep in mind that this is considered to be special category data and therefore merits a higher threshold of protection.



Very recently, the Hungarian data protection authority (NAIH) fined the office of Hungary's 11th District's Public Health Department the equivalent of €28,000 for failure to implement adequate protective measures for the transfer of data relating to COVID-19 rapid test results.

It became apparent that GPs in several Hungarian districts had inputted their patients' COVID-19 test results into an unsecured Excel sheet which was shared amongst various practitioners, enabling them to view health data of persons who were not their patients. Patient identity details were clear and even included details of other medical issues relating to them. To add salt to the wound, the database was transmitted around through the use of regular emails, without any standard of basic password protection or even encryption.

Whilst it was established that the Hungarian central health authorities had warned doctors of the importance of maintaining health data confidentiality, they still failed to take cognisance of this dangerous practice which posed a significant risk in case of breach and furthermore did not inform data subjects of said risk either. In fact, the warnings on confidentiality were found to be insufficient in terms of safety measures.

Sharing is Caring?

March 2021

On 2 September 2019, a patient had an MRI performed on his right knee at a hospital in Spain. A short while later, following a workplace accident on the same knee, his employer requested that he perform an MRI. This was carried out on 27 September 2019 at a different hospital. However, this hospital was owned by Affidea España, which company also owned the hospital at which the patient had carried out the first MRI.

It consequently resulted that whilst the hospitals were completely different entities despite being owned by the same company, the second hospital obtained information regarding the patient's first MRI from the other hospital without the patient's knowledge. In fact, his medical report clearly draws conclusions following analysis of the first MRI.

The company defended itself by firstly pointing out that its privacy policy indicates that the hospitals within the Affidea España group may share data to ensure accurate medical records, and that secondly its practitioners are duty bound to provide the most accurate results using all available data.

Due to this issue, the patient could not have his injury recognised as an occupational injury due to the first MRI (on the same knee) having appeared on the same medical report. Considering that this medical data had been transferred between the entities without patient authorisation (based on assumption), the group was hit with a fine of €10,000.

Brad's in Trouble

March 2021

The Electric Authority of Cyprus has very recently been issued with a fine of €40,000 for continued use of the Bradford Factor system.

The Bradford Factor is a commonly used model which helps organisations track employee sickness absence. The system is automated and uses a multiplier formula which issues a rating based on the frequency and length of absences. The rationale of the formula concludes that the higher the rating, the higher the potential disruptiveness to the organisation, thus

implying that shorter and more frequent absences are more disruptive than one single absence for a long period.

Αρχή Ηλεκτρισμού Κύπρου

It is interesting to note that this is not the first time that the Cypriot data protection authority has fined a company for use of the Bradford Factor without a legal basis for the processing of employee absence data. In fact, last year a collective fine of €82,000 was issued to three entities operated by the same group for use of the Bradford Factor. The authority had remarked that the continued analysis of employee sickness absence for human resource planning purposes was an illicit intrusion into one's privacy in relation to health data.

Whilst no other fines of a similar nature relating to the use of the Bradford Factor have been seen in other EU jurisdictions, due attention must be given to the reasoning expounded in this case.

Technical & Organisational Measures

Art. 31 GDPR - Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Health is Priceless, Right?

December 2020

Several healthcare providers (clinics and hospitals) in Sweden were issued with a variety of fines in December 2020, ranging from €244,000 to €2,900,000, in relation to inadequate technical and organisational measures in place to ensure the security of patient data.

Thorough inspections were carried out by the Swedish data protection authority on eight different healthcare providers in Sweden. The entities' patient medical record infrastructure and the access, retention and security measures in place on such systems were thoroughly studied. Seven out of the eight entities investigated by the authority were found to be in breach of the technical and organisational requirements laid down in the GDPR. These entities were found to have failed to perform regular data analyses and updates, whilst having no reasonable limitations in place with regard to staff's access to patient data.

The authority reiterated that the conducting of penetration testing is crucial when taking into consideration the rights and freedoms of the data subjects concerned, who in this case were patients whose medical (and therefore sensitive) personal data was being processed.

The fines varied depending on whether the healthcare facility was a private entity or a governmental authority or body, wherein the fine capping would differ. In fact, the two highest fines following the highest fine of €2.9 million were of €1,168,000 and €1,463,000.

Relationships

Marital Woes

April 2021

A financial institution in Belgium was slapped with a €100,000 fine when one manager accessed his wife's credit information without a legitimate reason at law, to gain an upper hand in their divorce proceedings.

The company permitted its employees two level of access to the Belgian National Bank's Central Credit Register, and access rights mainly based on their seniority. When managers accessed the Register, whilst their movements could be tracked on the system, it would not record their individual identity but would only register that a management team member is accessing it.

In fact, the Belgian authority dealt with a case wherein it had to investigate an individual from the management team who accessed a particular woman's file on the Register over 20 times within a period of two years. Whilst it was not possible to indicate the identity of this person due to the lack of identity tracking, the authority noted that one such manager was in the process of divorcing and liquidating his joint estate with his wife. Lo and behold, his wife just so happened to be the woman whose files were accessed on the Register.

In fact, the wife had filed a complaint before the Belgian authority, claiming that she suspected her husband had been accessing her credit register by abusing his position at work. This subsequently led to the authority investigating what measures the company had in place to ensure an appropriate level of security in relation to the risk of unhindered access to the Register without identity tracking for managers of the financial institution in question. The authority concluded that the exemption from identity tracking was a "blatant violation" in light of the type and nature of data accessible on the Register.

Interestingly, the wife had also submitted a complaint with the authority against her ex-husband personally besides the complaint against the company itself, however a decision on this is yet to be taken.

Wrong Number

January 2021

A patient was admitted to the gynaecology department of a hospital in Faenza to undergo abortion procedures, and upon discharge she specifically requested that she is only contacted on a specific phone number which she provided to the staff on duty at the time, and that no details regarding her medical procedures were to be given to any third parties.

A short while later, a nurse phoned the number she found on the patient's regular medical record. The patient's husband picked up, and she introduced herself as the nurse from the Faenza hospital gynaecology ward, but gave no further information. During investigations, the nurse confirmed that she had made the call because she had provided the patient with a drug and had not had the opportunity to inform her about its effect before the patient discharged herself from the hospital without the nurse's knowledge.

It was later revealed that the new number the patient had given had not been inputted into the computerised system and was only attached to the physical medical file, which the Italian authority considered to be an "inadequate [measure] to protect the dignity of the interested parties". The hospital was fined €50,000.

Parental Guidance

January 2021

An employee of a construction company in Spain had caused certain damages on a property during refurbishment works. The company proceeded to send a letter to the employee's father asking him to pay for the damages caused by his daughter.

During investigations, it was revealed that the employee's father had been an employee of the same company, which explained how it was in possession of the father's details. The Spanish authority considered that the processing of this data for this specific purpose was made without any legitimate justification at law, and therefore found the company in breach of data privacy law. The company was subsequently fined €3,000.

Recordings

Are You Recording Me?

August 2020

Online shoe retailer Spartoo was fined €250,000 by the French CNIL for several counts of personal data processing breaches, including the processing of recorded telephone conversations.

The company recorded each and every one of its call centre telephone conversations with clients for the purposes of quality control by company trainers, who only listened to one such call per week. This was strictly disproportionate and unjustifiable, especially considering that certain clients had passed on bank details and, in some cases, health card details via such telephone conversations. Clients could only be made aware of this by looking at the website privacy notice, which however did not provide a legal basis for such processing anyway. In fact, the authority further highlighted inconsistencies found in the company's website privacy notice, particularly in terms of its legal bases for processing of data.

The CNIL also found the company in breach of its data retention responsibilities, concluding that the company held data of over 3 million customers who had not even logged into their account within the previous 5 years. Further issues relating to security were highlighted wherein it was noted that clients were not encouraged to use strong account passwords.

The retail giant retained online presence in several EU states, and therefore affected citizens resident within several countries besides France. In this light, the CNIL also consulted with and requested the cooperation of several data protection authorities in such other EU states.

Subject Access Requests

Art 15 GDPR - The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

a) the purposes of the processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f) the right to lodge a complaint with a supervisory authority;
g) where the personal data are not collected from the data subject, any available information as to their source;
h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Hurdle Dash

July 2020

SARs are a headache, that's true. It's a mad task of sifting through endless emails and documents, redacting confidential information, preparing all data in an easily readable format and ensuring that all this is done within the time limit imposed. As enticing as charging a data subject making a subject access may seem, don't. The Dutch National Credit Register tried to do that and was fined €830,000 – not a good trade off at all.

The Register had been the subject of complaints submitted to the Dutch supervisory authority, wherein data subjects complained of the fee being requested of them when submitting a subject access request. During its investigations, the authority further noted that the Register imposed a further hurdle wherein it limited physical (paper) format requests to be made only once a year.

The Dutch authority confirmed that a data subject's right to make a data access request is, in fact, a right. This right is enshrined within the text of the GDPR and may therefore not be burdened with any further hurdles imposed upon the legitimate exercise thereof. The authority chairperson further highlighted the importance of this Register upholding this right in light of the fact that negative credit registrations may have detrimental effects on obtaining loans or mortgages.

Tick Tock

January 2021

A subject access request is a right at law available to the data subject. Therefore, following up on it in time is crucial. A January 2021 decision of the Italian Garante contemplated a fine of €2,000 issued to a company for failure to reply to a SAR in time.

Initially, the complainant's subject access request for access to his daughters' data from the health facility in question was completely ignored. Following this, he filed a complaint with the Italian authority, which imposed a 20-day limit on the company to reply to the complainant's request. The authority also reprimanded the company for the delay and ordered it to prepare an adequate procedure to address other claims of a similar nature.

The fine was nonetheless imposed as the Garante considered that whilst the subject access request was finally responded to, this was done 62 days following the date of the request and only upon its formal intervention.

Please Reply!

To date the highest fine under GDPR issued by the IDPC was when personal data undergoing processing was partially provided following a right of access request and the Privacy Policy did nt satisf the transparency requirements. This landed the Controller with a €20,000 fine. In another case, the IDPC issued a €5,000 fine after an entity failed to reply when it was asked for information following an access request. In another three cases the Controllers were reprimanded.

Cookies

A cookie is a small text file that is downloaded onto 'terminal equipment' (eg a computer or smartphone) when the user accesses a website. It allows the website to recognise that user's device and store some information about the user's preferences or past actions.

GDPR Goes Stateside

May 2021

Several Norwegian websites made use of a plugin which operates a public comment platform through Disqus, a US-based company. It was brought to the Datatilsynet's attention through several reports in the media that Disqus had been unlawfully tracking website user data and which websites they prefer to visit, which was then passed on to third party marketing entities.

Upon being faced with investigations, Disqus made it clear that it was unaware that the GDPR applied in Norway, which is not an EU member state. For all intents and purposes, whilst the Regulation was issued within the EU, it was made to also apply to EEA countries, which includes Norway. Nonetheless, the company attempted to justify the processing on the basis of its legitimate interest in terms of marketing, yet the Datatilsynet concluded that data subject consent was required nonetheless in this case.

Furthermore, not only did the company not seek data subject consent for processing of data for marketing purposes, but it also did not provide any information to users about the details relating to the tracking, profiling and disclosure of their data, making this form of tracking highly invasive.

Taking into account the fact that the company was not even aware that the GDPR applied in Norway in conjunction with the severely invasive manner in which the tracking was imposed, heavily lacking in transparency, the authority imposed a provisional fine of €25,000,000, which is subject to revision upon the company's comments which are to be submitted by the end of May 2021.

Unlawful Processing

Bank Lacks Interest to Comply

February 2021

Caixabank, one of Spain's largest banking institutions, has been hit with a €6,000,000 fine, the highest fine meted out by the Spanish authority at the time (now surpassed by a more recent €8,000,000 fine issued to Vodafone España in March 2021).

The Spanish AEPD found the bank guilty of breaches on two main counts. Firstly, its entire collection of privacy documentation was found to be lacking in several respects, such as with regards to what type and categories of personal data is collected by the bank and more specifically the reasons for which this data is processed. On these counts, the AEPD fined Caixabank €2,000,000, taking into consideration the nature, gravity and duration of the breach and the volume of client data involved and the scale of the company's operations and turnover, whilst also accounting for the negligent nature of these infringements.

The remaining €4,000,000 constituting the totality of the fine was issued as the authority found that the bank had never implemented a mechanism to obtain clients' consent for the processing of their data, but simply justified such processing on the basis of its 'legitimate interests'. Such interests were in fact not clearly defined in the privacy documentation above referred.

Supermarket Super Breach

November 2020

A €2,250,000 fine has been issued by the French CNIL to Carrefour France following lengthy inspections triggered by numerous complaints. Another additional €800,000 fine was issued to Carrefour Banque.

Initially, the CNIL considered the fact that Carrefour website privacy documents were not easily accessible, and were intermixed with several other unrelated information, therefore creating unnecessary impediments. The wording was therefore unnecessarily ambiguous. It was also noted that when one applied for a bank card with Carrefour Banque and wished to link it to Carrefour's loyalty scheme, one had to tick a box consenting to certain types of data to be transferred – the CNIL had no problem with the data listed as it was necessary for the purpose outlined. However, it was eventually discovered that several other types of data were transferred between the entities in reality.

Other breaches included automatic advertising cookies which were automatically enabled upon entry to the website, contrary to the reasoning expounded in the Planet49 case, which clearly highlighted the manner in which cookie consent should be enabled on websites upon access.

Carrefour was also found guilty of retaining data of over 28 million customers who had been inactive on the company systems between five to ten years. The data retention period of 4 years from the date of the last purchase was considered excessive.

Other breaches in relation to subject access requests were found, wherein the CNIL primarily determined that the request for proof of identity was an unnecessary imposition considering the fact that the online account was sufficient in itself. The company was also found to have defaulted in keeping with the legally imposed deadlines in several instances where requests were made, both for access, objection and deletion. Several objection and deletion requests were in fact ignored due to internal technical errors.

Problematic Policies

December 2020

Several complaints against Banco Bilbao Vizcaya Argentaria (BBVA) had been submitted before the Spanish AEPD wherein data subjects complained that they had not consented to receiving promotional messages through various means.

The Spanish authority made reference to BBVA's privacy documents and noted that the client would indeed consent to marketing by signing the same document. However, it resulted that to become a client of the bank, the document needed to be signed anyway and therefore the mechanism constrained the client to consent to receiving promotional ads to merely use the bank's services. The only way clients could opt out from marketing consent is by specifically ticking boxes to that effect. Furthermore, the AEPD concluded that one signature for the entire document could not be validly construed to apply to each and every purpose mentioned in the policy, particularly in terms of the manner in which such purposes were drafted.

The manner in which this policy is drafted was deemed to run strictly contrary to the spirit of the GDPR. Furthermore, the AEPD noted the rather imprecise and vague terminology used, for example that the client would sign on to the privacy policy for the bank to "get to know [the client] and better personalise [the client's] experience". This does not effectively state that the client would be receiving direct marketing communications, thus leaving a degree of ambiguity. This was also considered to be an illegitimate form of data subject profiling without any specified aim.

The AEPD also referred to the lacking detail in the bank's legitimate interest for and purposes of processing. The policy also defaulted in highlighting the specific types and categories of data which are processed by the bank, only providing vague descriptions of such categories of data.

In light of the above, the Spanish AEPD went ahead with imposing a €5,000,000 fine on BBVA for processing without a legitimate basis and in manners which ran contrary to the data subjects' fundamental rights and freedoms.

Thank You

First and foremost, we thank, you, the participants, we hope that you found the conference both informative and interesting.

A big thank you goes to Dr Patrick Farrugia from 21 Law who carried out most of the research which made it possible for us to present and discuss the cases during this conference and to Gabriella Farrugia who helped in he research.

We cannot miss thanking the Information and Data Protection Commissioner, Dr David Ciliberti from the European Commission, Mr Axel Voss, MEP and Dr Sarah Cannataci from Fenech and Fenech Advocates.

We hope to see you all back at the conference next year... we will remind you about it, unless you exercise your right to be forgotten 😜