CONFERENCE NOTES

Supported by

Contents

Welcome to the *GDPR - Two Years On* conference

Not in a million years would I have thought that our annual conference would be held online but who would have thought that the world would have had to face the COVID-19 pandemic - a pandemic which also had an impact on GDPR because the advice had to be tailor-made to this specific circumstance. In this second year we have learnt so much more, and nothing beats reviewing and assessing cases happening locally and in Europe.

It is these cases which bring the law to life and why we organise this conference. We want to keep you informed and updated on the various developments and interpretations of data protection.

We saw massive fines and cases which confirm how the law has been implemented, as well as cases which teach us what we need to do going forward.

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, the valuable speakers, and our main sponsor CyberSift.

May you enjoy our conference despite it is being online and thank you for your participation.

We truly appreciate it.

Roselyn

Programme

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

09.30 - 09.45 **Two 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 **Cyber Security** - *Mr Brian Zarb Adami CyberSift*

10:55 - 11:30 **Case Law review (Foreign)** - *Dr Roselyn Borg, 21 Law & Dr Sarah Cannataci, Fenech & Fenech Advocates*

11.30 - 12.00 **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 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.

His first tasks were to assist the Commissioner on capacity building and on the implementation of the new set of rules which introduced fundamental rights to data subjects and imposed obligations on data controllers. At the time, the careful implementation of structured efforts was indeed necessary to bring along a smooth culture change in the manner personal data were processed by both the public and private sectors.

During the years, Ian has acquired a level of expertise in data protection. Currently, he holds the position of Deputy Commissioner where his main areas of responsibility include the investigation of data protection complaints and personal data breaches, advising the Commissioner on various local and European data protection issues and other technological matters, conducting on-site inspections and investigations, actively participating in European working groups on data protection and devising the necessary policies and strategies for the effective enforcement of the Regulation.

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 is currently widening his horizons by studying Liberal Arts and Sciences at the University of Malta and a Masters in Business Administration.

Mr Brian Zarb Adami

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. The highest among these resulted from a decision of the UK's Information Commissioner's Office (ICO) in July 2019 in the amount of **€204,600,000**. British Airways were slapped with this monumental fine which shall go down in GDPR-history for having negligently allowed its website's users to be diverted to an unauthorised website. By consequence of this, half a million customers ended up giving out their personal data to hackers, including bank card details.

The second highest fine to date ran into the amount of **€110,300,000**, handed down to Marriot International (also by the ICO) for having failed to carry out sufficient due diligence when acquiring Starwood Hotels in 2016. A cyber-attack had previously occurred on Starwood's website which Marriot was unaware of, with 339 million guest records (including encrypted passport numbers) having been compromised. Around 30 million EEA residents' data was included therein.

Other significant fines included the **€50 million** penalty handed out by the French authority (CNIL) to Google, which we discussed in depth in our first GDPR conference held last year. The fine was imposed as the CNIL concluded that Google failed to provide sufficient and clear information to users about its data processing.

The Italian and Austrian authorities handed out **€27.8 million** and **€18.5 million** respectively in fines for other data violations, the former regarding Insufficient legal basis for data processing and the latter for unsolicited trading of consumer data, thus cementing the states' authorities place in the top five highest fine statistics under the GDPR. More information about both cases can be found in page 21 and page 25 respectively.

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

Country	Fine	Entity	Type of Breach
United Kingdom	€204,600,000	British Airways	Insufficient technical and organisational measures to ensure information security
France	€50,000,000	Google Inc.	Insufficient legal basis for data processing
Italy	€27,800,000	TIM	Insufficient legal basis for data processing
Austria	€18,000,000	Austrian Post	Insufficient legal basis for data processing
Germany	€14,500,000	Deutsche Wohnen SE	Non-compliance with general data processing principles
Sweden	€7,000,000	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	€645,000	Morele.net	Insufficient technical and organisational measures to ensure information security
Portugal	€400,000	Public Hospital	Insufficient technical and organisational measures to ensure information security
Norway	€283,000	Bergen Municipality	Insufficient technical and organisational measures to ensure information security
Spain	€250,000	Professional Football League (LaLiga)	Insufficient fulfilment of information obligations
Denamrk	€200,800	IDdesign A / S	Non-compliance with general data processing principles
Greece	€200,000	Telecommunication Service Provider	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
Finland	€100,000	Posti Group Oyj	Insufficient fulfilment of data subjects rights
Hungary	€92,146	Organizer of SZIGET festival and VOLT festival	Insufficient legal basis for data processing
Ireland	€75,000	Tusla	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
Belgum	€50,000	Social Media Provider	Insufficient legal basis for data processing
Slovakia	€50,000	Social Insurance Agency	Insufficient technical and organisational measures to ensure information security
Iceland	€20,600	National Center of Addiction Medicine ('SAA')	Insufficient technical and organisational measures to ensure information security
Czech Republic	€10,000	Unknown	Non-compliance with general data processing principles
Malta	€5,000	Lands Authority	Insufficient technical and organisational measures to ensure information security
Estonia	€500	Housing Association	Insufficient legal basis for data processing

[1] Source: GDPR Enforcement Tracker

Cases in Malta

Silence is Golden

February 2020

Daniel Zammit v Rocco Bartoloccio (Tribunal ghat-Talbiet Zghar)

FIT - TRIBUNAL GHAL TALBIET ZGHAR
SMALL CLAIMS TRIBUNAL

In a recently handed down decision of the Small Claims Tribunal, the presiding adjudicator determined that covert recordings can be admissible as evidence in court.

The plaintiff (Zammit) brought forward certain pre-recorded telephone conversations to be approved as evidence during proceedings. This request was vehemently slammed by the defendant (Bartoloccio), who contended that such recordings were not to be admitted and were to be deemed inadmissible as they had been taken without his consent.

The Tribunal delved into deep considerations as to the admissibility of evidence in Maltese courts as determined in local jurisprudence. The decision points out that the American exclusionary rule, which forbids the use of illegally obtained evidence in proceedings, does not apply in Malta. In fact, local courts follow the English model, which is more heavily based on the rules of relevance and best evidence rather than the legality with which such evidence 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.

The decision even goes on to quote a previous case (Raymond Cutajar vs. Grand Hotel Excelsior), which highlights in plain language that persons have a right to record conversations for the purposes of retaining evidence of what happened, and the fact that this is done covertly cannot render the recording inadmissible as evidence in proceedings. However, the Tribunal noted that the defendant was still within his rights to file a report with the Information and Data Protection Commissioner (IDPC). Nonetheless, if the Commissioner deems the recording to have been illegally obtained in terms of data privacy law, it would still be admissible in proceedings in terms of relevance.

Mother knows best

June 2020

George Buttigieg vs. Rebecca sive Becky Zarb Gauci Maistre (CoA Inferior)

The decision of an appeal from the Court of Magistrates handed down very recently has seemingly overturned the line of thinking which has been made clear in the previous decision discussed above.

Qorti: TA' L-APPELLI CIVILI (INFERJURI) - QORTI TA' L-APPELL
Gudikant/i: ONOR. IMHALLEF LAWRENCE MINTOFF
Appell Civili numru: 199 / 2011

The case at hand aimed to decide a case of libel and defamation allegedly made via email communications. In simple terms, the plaintiff (Zarb Gauci Maistre) had sent an email to Parentcraft (Mater Dei's midwifery unit, aimed at caring for and helping new mothers). This email referred to the plaintiff's gynaecologist in a rather negative light, and its content subsequently escaped Parentcraft's realm (circulating amongst certain nurses) and ended up on the lap of the same gynaecologist - the plaintiff (Buttigieg).

The Court of Magistrates initially concluded that email communications are not necessarily private in nature, reprimanding the defendant and claiming that she should have been wary of sending such delicate information via email. This is because the content thereof could easily be made public, both by the recipient or third parties in possession of it (as happened in this case). The court therefore admitted the email as evidence.

The disgruntled mother appealed, claiming that since she had sent the email to the specific hospital unit aimed at assisting new mothers, the recipients (midwives) were bound by professional secrecy and could therefore not divulge any content received. The appellate court welcomed the appeal and concluded that the email was in fact illegally obtained and should never have even left Parentcraft's sphere of control, thus impugning the first judgment which accepted the plaintiff's claims.

Yours, mine & ours

June 2020

LeoVegas Gaming p.l.c. vs. the Commissioner for Information and Data Protection (CoA Inferior)

In another case, also very recently decided, the court engaged in a heated issue regarding the ownership of data in terms of marketing strategies. Several persons in the UK had complained to the ICO that they were receiving unsolicited marketing messages from LeoVegas, a gaming company registered in Malta, and the ICO asked the local IDPC to investigate.

LeoVegas appealed the IDPC's decision to hand down a €5,000 fine for breach of data privacy law before the Data Protection Appeals Tribunal, which appeal was rejected. LeoVegas went on to appeal the decision before the Court of Appeal. It claimed that since the marketing occurred via a UK promotions affiliate, which advertised the casino's services, LeoVegas could not be held to be the data controller as the data processed by the affiliate was solely collected and processed by it, and thus LeoVegas could in no way hold itself out to be the owner and controller of such data.

However, in spite of the above, the appellate court concluded that the IDPC had been correct in concluding that LeoVegas was in fact the controller in this case. This was determined based on the fact that the marketing activities were directly commissioned by LeoVegas (which company had provided the affiliate with the promotional material to be used and also had a say in the manner in which it was to be marketed). As the instigator of the marketing campaign, LeoVegas was thus considered to be the controller by the court and therefore the fine was justified in this light.

Central Bank admonished

February 2020

In early 2020, the Central Bank of Malta was caught in the midst of a data breach for which no fine has been meted out, but the institution was nonetheless served with a reprimand as a warning to both itself and all other institutions handling personal data.

In this case, a former employee of the Central Bank brought forward a complaint before the IDPC, claiming a breach of his privacy rights. In 2019, this individual had been dismissed from the institution on disciplinary grounds. However, during the investigations the claimant argued that the Central Bank had violated the provisions of the GDPR. In essence, he made four separate allegations.

Firstly, the ex-employee claimed that the Central Bank had notified its union's president that he was being suspended during the investigations without his consent. In fact, the collective agreement provides that the union is to be made aware of the conclusion of proceedings, and no data in this regard should be disseminated prior to that.

The complainant had also claimed that the bank had divulged his personal data vis-a-vis his application for the Governor's Award, when an email was erroneously sent out to all applicants without using the blind carbon copy ('bcc') function. Ironically, this was the same data which the individual was accused of mishandling. Whilst the latter was recognised as a violation from the Bank's end by the IDPC, the Commissioner noted that a report drafted on the same misuse pointed out deficiencies of Central Bank in terms of data access security was insufficient to prove that the ex-employee's data privacy rights had been breached in this regard.

The complainant had however alleged that his request that the Central Bank erases his personal and union data was unduly declined. He also claimed that he had been coerced into permitting the Bank to access his computer and email account. The IDPC found that this course of action was permissible in terms of conducting a thorough investigation into the alleged misconduct.

Snooping bank made to pay

August 2019

A major banking corporation has been slapped with a €5,000 fine by the IDPC in August 2019 for a serious breach of an employee's privacy rights through an abuse of its position. In this case, an employee had request to switch to working on a part-time basis for some time. An agreement was signed between the parties, laying down certain conditions which had to be observed.

In 2017, the bank qua employer began suspecting that the employee was not upholding his end of the bargain. Bank officials subsequently began monitoring the employee's personal accounts (which were held with the same bank) to assess whether he was receiving any additional income over and above his salary in violation of the agreement signed by them.

Whilst the bank itself had access to the accounts because it was in fact the data controller in that regard, the monitoring was found to be illegal by the IDPC as a distinction had to be made between how the bank could use its powers vis-à-vis the complainant in his capacity as an employee, and as a private individual who chose to hold a private account with the bank. In using one situation to benefit the other, the bank was found to be strictly in breach of the law as it had no legitimate interest in monitoring the individual's income for employment purposes in this case.

International Cases

The international cases are grouped by the type of data breach. Not all of the cases will be discussed during the conference but we thought of having them here for those who would like to go through them.

Inadequate Security, Technical & Organisational Measures

Do-not-call means do not ever call me

October 2019

Greek telephone service provider fined for inappropriate technical measures and errors

The Hellenic Data Protection Authority fined a telecom provider (OTE) a total of €400,000 on two counts relating to technical faults and errors in the company's systems.

On one hand, various subscribers of the company had been receiving unsolicited marketing calls from third companies, despite them being listed on the 'do-not-call' register. This generally resulted from cases of clients who made a data portability request upon changing provider. Upon making the request, their data was cancelled from the 'do-not-call' register. However, in cases where the request was subsequently cancelled, the procedure for the restoration of the data was not regulated internally. Therefore, clients cancelling their request were not placed back on the 'do-not-call' register once their data had been deleted off it, consequently infringing the principles of data protection by design and the principle of accuracy under the GDPR.

The second infringement consisted in a repeated system fault stretching back to 2013, which only came to light following a number of years upon several complaints being made. OTE's clients had been receiving advertising messages, despite having unsubscribed therefrom. However, persons who unsubscribed via a specific link were still receiving messages due to some error in the same link. Therefore, the Hellenic Authority concluded that OTE lacked the appropriate technical measures to detect such faults.

DPOs: Conflict of interest is a no-go

April 2020

Proximus, Belgium's largest telecommunications service provider, has been slapped with a €50,000 fine on grounds of appointing a data protection officer (DPO) with a significant conflict of interest. The GDPR provides that the DPO, as the appointed person responsible for ensuring compliance with data privacy law and the protection of personal data processed by a data controller, must be protected from any sort of conflict of interest.

In the case at hand, it was discovered that Proximus had appointed the director of audit, risk and compliance as the DPO. The authority argued that due to the operational nature of these roles (especially since there were multiple ones) there may arise a situation of self-monitoring, which would result in the envisaged conflicts. Guidance suggests that, in general, an in-house DPO should be disallowed from interfering in data protection matters affecting one's own department, especially if holding a role of significant importance. This issue was perpetuated in the current case by consequence of the fact that the DPO held multiple directorship functions. Further to the above, it resulted that the DPO was not being actively involved in data privacy matters by the company itself, constituting further non-compliance with the law.

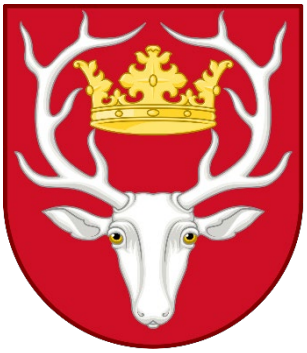
Moreover, the Belgian authorities became aware of this infraction during investigations being carried out following a data breach which the company itself had brought to the attention of the authority. This therefore highlights the importance of ensuring that all adequate measures are in place, as a breach in one area may reveal significant flaws in others. In fact, whilst Proximus was handed down the fine on the issue relating to the DPO, no sanction was issued with regard to the self-reported breach.

Stolen computers cost towns more than they thought

March 2020

In March 2020, two separate incidents of theft of technical equipment owned by Danish municipal authorities resulted in potential significant data breaches, for which the two authorities were fined by the Danish Data Inspectorate (Datatilsynet).

In Gladsaxe, a computer had been stolen from the city hall. The computer contained the personal data of over 20,000 persons, covering items such as names and identification document numbers and also other, more sensitive kinds of information. On the other hand, the Hørsholm municipality was handed down a fine when an employee's laptop was stolen from his car, which laptop contained the data of around 1,600 employees of the authority. Amongst this information was included the employees' social security numbers together with other categories of sensitive data.



The Gladsaxe authority was fined €14,000, whilst Hørsholm was fined €7,000. The Datatilsynet noted that the significant fines resulted from the fact that municipalities are responsible for processing a significant amount of data, which regularly also includes sensitive information, of its residents. Furthermore, the severity of the breach resulted from the fact that neither the computer nor the laptop were encrypted. Therefore, access to the data contained in either one was fairly easy by accessing the hard drive through another device. The head of the Danish supervisory authority branded the lack of protection as "extremely careless".

Calm after the storm? Not likely

December 2019

The UK Information Commissioner's Office (ICO) has delivered a fine to a pharmacy for the lack of basic security practices which aimed to serve as a lesson for all data processors as to the importance of providing adequate security and storage measures.

The investigation came about following the ICO being notified by the Medicines and Healthcare Products Regulatory Agency, which was conducting its own investigation into the pharmacy's operations. The documents, which contained a great deal of personal client information (including sensitive information considering the nature of the company's business, such as NHS numbers and medical information), had been left in unsealed containers without any form of protection. The containers consisted in several crates, a cardboard box, and two disposal bags. These

containers had been left in the pharmacy premises' courtyard, which was accessible from the overlying residential apartments via a fire escape.

The Director of Investigations of the ICO commented that storage of hard copies of documents without envisaging adequate measures of protection thereof was extremely "careless", especially considering the sensitive nature of the data contained therein. Furthermore, the few policy documents which the pharmacy had in place to regulate the handling of data were inadequate, in template format, and had clearly not been updated since 2015, and therefore since before the entry into force of the GDPR. The ICO furthermore raised concerns about the retention of the data, some of which stretched back to 2016.

Elementary security flaws cost company €10 million

December 2019

The German Federal Data Protection Authority (BfDI) has handed out its second highest fine to date, amounting to €9.55 million, to 1&1 Telecommunications for failure to implement sufficient technical and organisational measures to secure its clients' data in terms of authentication.

The German telephony service provider, one of the country's largest, had been freely providing personal information via its customer service hotline, so long as the caller provided the client's name and date of birth. The BfDI slammed this procedure as excessively insufficient to adequately protect the integrity of clients' personal data.

Whilst commending 1&1 for their transparency, cooperation and willingness to take steps to implement more effective security measures, the BfDI felt that the imposition of the fine was nonetheless necessary to serve as a deterrent, despite the authority reporting that the fine was on the lower end of the spectrum. Further to this, whilst a small portion of customers were actually affected, the potential risk of infringement extended to "the entire customer base", so long as the caller could identify them by their name and date of birth.

Multi-factor, or multi-fine

October 2019

UWV (Employee Insurance Agency) has been slapped with a monthly fine of €150,000, amounting to a maximum of €900,000 in total, for failure to implement adequate multi-factor security measures for access to its employee portal.

The online portal, which contains detailed information on employees, also covers their sick leave records (which the Dutch authority classified as 'health data', thus constituting sensitive data which merits a higher level of protection). The authority found the portal security system in place at the time significantly lacking in terms of safety. Whilst UWV had taken certain additional security measures, the authority continued to emphasise that these were insufficient in isolation if they were not together incorporated with a multi-factor authentication system.

This form of authentication has become increasingly popular in recent years, as it offers persons accessing any form of online portal the benefit of confirming that they are the authorised data subject. Upon logging in, one receives an additional confirmation (such as an authentication number) through another account such as email, or on another device such as a mobile phone. This provides an added layer of security, thus protecting the integrity of the sensitive data contained on UWV's portal.

A delay in the company's installation of the system was noted, but it was largely based on third party delays, on whose action UWV depended for the implementation of the system, rather than inefficiency of the company itself, which in fact acted with haste to rectify the issue.

Direct Marketing

Game, set and ...fine?

March 2020

The Dutch Data Protection Authority slammed the Royal Dutch Lawn Tennis Association with a hefty administrative fine after having sold the personal data of approximately 350,000 of its members to two of its main sponsors. The categories of data included direct contact details (such as addresses and phone numbers) which were used by the sponsors in question for direct marketing, mainly for offers relating to tennis equipment.

The Association attempted to justify itself by claiming that it had informed all members of its intentions via a newsletter and also through its website. This justification could however hold no water, as no direct consent had been given by the members whose data had been sold.

The Dutch authority made a distinction between the member data collected prior to 2007, and from 2007 onwards. In the first category, the data had not at all been collected for any specific marketing purposes or activities, even if in relation to the Association's sponsors. Therefore, there is no direct link between the original intention of the collection of the data and the direct marketing purposes for which it was subsequently used, and thus obtaining the members' consent had been undoubtedly necessary. With regard to data collected after 2007, the authority recognised that from then on, the Association began to collect data for purposes of furthering income. However, it determined that this could not be relied upon as a ground of 'legitimate interest', as this interest must emanate from a fundamental right safeguarded by law, and not a commercial interest as in the case at hand. Considering this, together with the fact that the 'marketing' intent had not been clarified from beforehand prior to members providing their data, the authority concluded that consent for direct marketing should nonetheless have been obtained.

€27.8 million out of pocket - if only they had asked first!

January 2020

Following violations of data privacy law via the unlawful dissemination of data for marketing purposes affecting millions of subscribers, TIM SpA was fined a staggering €27.8 million, the fourth highest fine to date since the introduction of the GDPR in 2018.

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. In several cases, certain persons who were being contacted were not even clients of the telecommunications service provider, whilst one specific case saw a person being contacted 155 times within one month. It was also reported that the company held client data of telephone operators which engaged TIM as network provider, which data was being used for marketing purposes without the clients' consent. 20 separate corrective measures were imposed on TIM, effectively banning the company from making use of the data of clients who had not consented to direct marketing.

Following a thorough investigation conducted together with the state Financial Police, it was brought to light that countless promotional calls had been made to contacts via call centres appointed directly by TIM to contacts, irrespective of whether or not they had not consented to direct marketing. It was also revealed that these call centres ran severely unchecked by TIM, resulting in their repeated failure to update their contact lists (which lists did not match the ones held by TIM itself) and therefore illicitly retaining inaccurate or irrelevant data for much longer than necessary.

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. The use of data provided thereby has thus been prohibited via an injunction issued by the authority, whilst TIM has also been ordered to reconsider this scheme in this light.

Cold calling lands company in hot water

November 2019

In November 2019, the French National Commission on Data Freedom (CNIL) handed down a fine of half a million Euro to French company Futura Internationale for significant violations of the provisions of the GDPR in relation to unsolicited marketing campaigns.

In early 2018, the CNIL had received a grievance from a disgruntled customer who complained that Futura Internationale had been calling him repeatedly for direct marketing purposes, despite having repeatedly opted-out. Upon commencing investigations, the CNIL remarked that Futura Internationale was committing a staggering amount of violations in this regard.

The company subcontracted several call centres in Africa which processed customer data of a sensitive nature (health related) without the adequate safety measures for transferring such data across borders, let alone outside the EEA. There existed a number of contracts for this specific purpose, yet they were largely still in draft format and were in line with the law of the receiving country rather than the GDPR, contrary to the provisions of the Regulation. The company was furthermore violating data subject rights by recording telephone calls without notifying them before, whilst the data minimisation principle was consistently being overlooked as the entity was making and retaining both unnecessary and offensive comments about clients.

In terms of cold calling, the CNIL remarked that the company had repeatedly failed to inform its clients that they would be subject to aggressive marketing strategies. The authority opined that informing clients of the direct marketing they would be subject to once their data has already been collected without obtaining their consent was not sufficient. An adequate and uniform opt-out mechanism was largely inexistent.

Data Retention Policies

Forgot to spring-clean? That will cost you

November 2019

The Berlin Commissioner for Data Protection and Freedom of Information fined real estate company Deutsche Wohnen SA for inadequate systems for storage of tenants' personal data. Whilst the Commissioner concluded that the company had no legal grounds upon which to process its tenants' data, particularly in terms of its necessity, it also noted that there were serious cases of over-retention of personal data.

Deutsche Wohnen failed to implement a data retention policy in terms of the GDPR, which is meant to regulate the periods of time for which certain categories of data must be stored. Retention policies may also refer to safe and secure methods of erasure of data upon termination of the respective retention periods, unless other policies regulating erasure exist. In this case, Deutsche Wohnen had been urged to amend its retention system in 2017 during an inspection by the Commissioner, and this prior to the introduction of the GDPR. However, during a subsequent inspection in 2019, the Commissioner noted that whilst the company had acted in some regards, it still defaulted in implementing adequate data retention measures. In issuing the €14.5 million fine, the Commissioner considered that the company had no legal grounds to retain the personal data for longer than was necessary. This constituted an infringement of the GDPR's data protection by design' requirements, and that this was also an infringement of the general data processing principles as set out under Article 5 of the GDPR.

Unlawful Processing of Personal Data

Postal service gets itself into trouble: €18 million in the mix

October 2019

Österreichische Post AG (ÖPAG), an Austrian postal service provider, has been handed down a significant fine by the Austrian data protection authority. The authority concluded that ÖPAG had unlawfully processed personal data of its clients based on their alleged political affinity, which goes beyond the scope of why this data had been originally collected at the outset. This data was subsequently sold to a third party.

The authority further noted another breach of data privacy law, wherein ÖPAG had been processing its customers' package posting habits and the frequency of relocations. This data was directly used for marketing purposes. Whilst the processing of data in this manner is not strictly prohibited under the GDPR, however the purposes for which it was processed in this specific instance were illicit.

CCTV Monitoring

Got 'em!

October 2019

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

After noticing significant discrepancies in sales figures amounting to €82,000 in losses over a number of months, a supermarket manager launched an investigation and installed CCTV cameras. Whilst employees knew about the visible cameras, the manager also installed covert cameras of which the employees were unaware. Covert footage caught Lopez Ribalda (the applicant in this case) and other members of staff allowing customers to leave with unpaid items and stealing goods themselves.

Lopez Ribalda pursued an unfair dismissal claim against her employer, claiming that her privacy rights had been violated by her employer. She argued that her right to privacy under the European Convention of Human Rights (Article 8) had been breached, which argument was rejected by the Spanish courts.

Upon appealing before the European Court of Human Rights, the first instance decision concluded that the use of covert cameras breached the employee's right to privacy. However, upon appeal from the Spanish Government, the Grand Chamber concluded that the covert surveillance was in fact justified and proportionate. The Court considered that:

- the scale of the theft and the number of persons involved was rather significant;
- the surveillance was temporary and for a short period of time
- the covert cameras were placed in an area of the supermarket where privacy could not be reasonably expected anyway
- the number of persons who had access to the footage were limited
- the objective of the covert recording was for a strict security related purpose, and it was not appropriate to have informed the staff of it beforehand
- there were no less intrusive ways to catch theft in the supermarket

Lights, camera... violation?

October 2019

The Hungarian authority (NAIH) imposed a fine of 5 million Hungarian florins (approximately €15,000) on the Kerepes municipality for unlawful processing of data via CCTV surveillance inside a public building.

The NAIH considered that the Kerepes municipality had been illegally processing the data collected via the surveillance cameras as there was no legal basis to do so, especially considering the length of time over which the data was collected. The municipality's justification for the processing of this data was considered to be too broadly defined, and so the basis for the processing was not proportionate to the violation of the data subjects' rights. Therefore, the reason for installing CCTV surveillance must be rather specific and justified in terms of potential data subjects' privacy and on the basis that these rights may be overridden.

Lastly, the NAIH concluded that the Kerepes municipality was also in breach of its accountability obligations, as there existed no documentation regarding the CCTV monitoring, processing and storage of data and what happens to the data upon deletion, if it even occurs.

Beware: data on the loose

April 2019

The Norwegian Data Inspectorate (Datatilsynet) has issued a fine to foodstuff retail giant Coop Finnmark SA after footage of four teenagers shoplifting from a specific store had been sent to a person without authorisation to view it, from whose mobile phone the movement of the footage could not be tracked any further by the data controller.

The manager of the specific store where the incident had occurred had been reviewing the CCTV footage, noting four adolescents of between 15 and 16 years of age, two of which committed minor theft whilst the other two kept watch. The manager filmed the footage with his personal mobile phone and sent it to a friend of his (who was not in any way related to the store or its management), asking her if one of the boys was her son. From then on, control

over the data contained in the footage was lost by the controller. In fact, the acquaintance in question passed the footage on to her son, who then passed it on to other parties including other individuals who appear in the footage.

In considering the €36,800 fine, the Datatilsynet considered that the infringement was significantly basic and whilst it could have easily been avoided, it could have posed a serious threat to the data subjects' rights and freedoms. It also considered the fact that children had been involved in the footage disseminated, whose data requires an even higher threshold of protection, especially when it places them in a compromising position as offenders.

Not everyone is born to shine on camera

December 2019

Entirely Shipping & Trading SRL has been fined in the equivalent of €5,000 for violating employees' inherent privacy rights through excessive CCTV recording, specifically in certain areas where such recordings were strictly unnecessary.

Employees had complained to the Romanian National Supervisory Authority that the CCTV surveillance, which also captured audio recordings, covered various areas where the employees regularly worked. Office audio-visual coverage was deemed intrusive to employees' privacy as it processed footage where employees would be consistently present for a significant number of hours of each working day. Moreover, surveillance cameras were also installed in locker rooms, where employees kept their spare clothes and often changed. This was furthermore considered to be a significant intrusion of their privacy rights, whilst also running contrary to the principle of data minimisation.

The company failed to provide a legitimate interest for having installed the CCTV system. The Romanian authority also remarked that no trade union or employee representative had been consulted prior to the introduction of the surveillance system, nor were the proper documented policies in place. In addition, no data protection impact assessment had been conducted prior to the installation of the monitoring system.

It should further be noted that a separate fine of another €5,000 was issued to the same company since, during the same period, it had implemented fingerprint scanner access points to various areas of the company premises, which was strictly unnecessary and intrusive to employees' inherent data privacy rights.

Private Person Issues

Do not be fooled by the uniform

May 2019

The Baden-Würtemberg Commissioner for Data Protection and Freedom of Information (LfDI) fined a police officer €1,400 for having unlawfully abused of his position to obtain data to which he was not officially entitled.

The officer in question made use of his official user ID on the German Federal Transport Authority's traffic information database to retrieve data on a specific vehicle owner by using the vehicle's licence plate number. With the data retrieved, he conducted an automated identity request, from which he obtained the vehicle owner's personal details, including his landline and mobile phone number, and then proceeded to contact him.

Whilst the police officer was making use of the official credentials attributable to his post to obtain the above data, the purpose was of a strictly private nature. Therefore, the infringement could not be attributed to the officer's department as this action had not taken place in the course of his official duties. Therefore, the fine was imposed directly upon the officer.

Lewd photographer gets more than he bargained for

March 2020

In a very rare kind of decision under the current European-wide data privacy regime, the Spanish Data Protection Authority (AEPD) handed down a fine to a private individual for breach data privacy legislation.

In this case, a private individual had been taking photos of female bathers sunbathing or showering by the riverside in Valladolid, a number of which were also adolescents. The photos were captured for explicitly lewd purposes, and without the data subjects' (i.e. the women's) consent. The AEPD noted that whilst today images of public areas can easily be captured, what with practically each person having in hand a mobile device which can take photographs, the photos in question and the

subjects thereof were not obtained as a "result of chance", but with active conduct. Furthermore, the AEPD considered that through the images, the data subjects could easily be identified.

Despite the individual having attempted to justify himself by stating that the women in the photographs were his 'cousins', the AEPD handed down the €4,000 sanction to the individual. The fine was issued for breaching the women's inherent data privacy rights by capturing images of a sensitive nature without their consent, to be used for sexual purposes, especially whilst making other lewd acts on his own person in a public area whilst capturing the images.

Cookies

Cookies & choices

October 2019

The Spanish Data Protection Authority (AEPD) imposed a £30,000 fine on Vueling for failure to adhere to established rules on website cookie banners. The website's cookie banner offered detailed information on the kinds of cookies were being used by the website and that third-party analytic cookies could also be used.

However, the user was not offered the possibility to manage these cookies directly, but instead was informed that this must be done via the browser's settings. The banner should contain the options to reject or enable all cookies, or at least the possibility for the user to manage individual cookie preferences. The AEPD concluded that whilst the browser settings for cookie configuration are in themselves adequate, they do not allow the user to configure cookie preferences as per the provisions of the Planet 49 judgment by the European Court of Justice in October 2019. The latter decision, which was handed down a short while prior to the decision at hand, established a number of principles which must be observed on website cookie banners.

Employee Issues

Airline employee goes rogue

November 2019

Romanian airline TAROM was fined €20,000 by the Romanian National Supervisory Authority when one of its employees accessed the personal data of a number of the airline's clients via the company's booking app and published it online.

The Authority determined that not only was the publication a breach, but the employee's access to the passenger list was furthermore unauthorised. A question which often arises in cases such as this, is, why the employer (the airline, in this case) was sanctioned for the breach, and not the individual employee.

The Romanian Authority pointed out that the employer (as the data controller) was responsible for implementing adequate technical and organisational measures to ensure that its employees adhered to data protection legislation - this is regularly effected through written policies or training sessions, to mention a few examples. In this regard, the employer had failed to act and therefore the Authority concluded that it was to blame for the breach as the employee had not been adequately informed on the data protection limitations applicable in his regard.

They are sick of it

October 2019

The Cypriot Commissioner for Personal Data Protection has handed down a fine (split up amongst 3 separate companies of the same group) amounting to a total of €82,000 for illegal processing of employee data through a widely recognised human resources model. A total of 818 employees were affected across the three entities.

$$B = S^2 \times D$$

where:

- B is the Bradford Factor
- S is the total number of spells (instances) of absence of an individual over a set period
- D is the total number of days of absence of that individual over the same set period

The Bradford Factor is a popular tool used by numerous companies, both locally and abroad, to monitor employee absences. The general theory behind the tool concludes that frequent, irregular absences for short periods of time pose a greater organisational burden on a company than longer and occasional absences from work.

The employers in question were using the Bradford Factor to specifically monitor sick leave by feeding the relevant data into an automated system and consequently profiling employees of each company by scoring them through the factor's result scheme. The authority however considered that employee sick leave records are considered to be special category data, and therefore classifying and profiling employees on the basis of sick leave was certainly not within the employer's right as it was not at all necessary for the organisation or control of the company. The authority went so far as to claim that in so doing, the employer would furthermore be wearing the hat of a medical professional, potentially leading to punishment being affected on a discriminatory basis. The use of the Bradford Factor could in no way be justified on the pursuance of the company's legitimate interests, as they could in no way outweigh the employees' privacy rights and freedoms.

Email Accounts

My emails, my property?

January 2020

In January 2020, the Hungarian authority (NAIH) imposed a fine on an employer for failure to provide adequate internal policies, intended to lay down strict rules and guidelines for the purposes of adherence to data privacy laws.

A fine of €1,500 was handed down to the employer in question for having restored the archived email account of a director who had previously left the company. The employer's intent was to search for a specific legal document, yet in processing the data contained in the mailbox, also went through potentially private information. The ex-director complained that this act breached his privacy rights, as he had been given no previous warning of the reactivation of his mailbox, and therefore had no opportunity to delete or retrieve any private information contained therein.

Here, the NAIH nonetheless noted that an employer is not strictly prohibited from performing the above actions, especially if it is in the employer's interest to do so to prevent or mitigate any potential integrity risks (so long as it is proportionate to the privacy rights of the employee). However, it is a rule of thumb to inform the employee in question of the potential restoration of the account. The NAIH went so far as to recommend that the employee should also be present whilst the data is being accessed (if reasonably practicable), or should at least be given the opportunity to do so, and that the access should be recorded.

Biometric Data

Fingerprint access: employees point out the invasion of privacy

May 2020

The Dutch Supervisory Authority has handed down a fine of €725,000 to an employer for implementing an access and time management system operated via fingerprint.

Upon becoming concerned with employee fraud in the employer's previous time management and attendance system operated via ID badges, a fingerprint scanner was installed. Following a complaint being brought forward by an employee, the Dutch authority noted that since biometric data is considered to be highly sensitive data, it may only be collected on condition of explicit consent of the data subject and for specific security purposes. The employer however failed to satisfy both requirements.

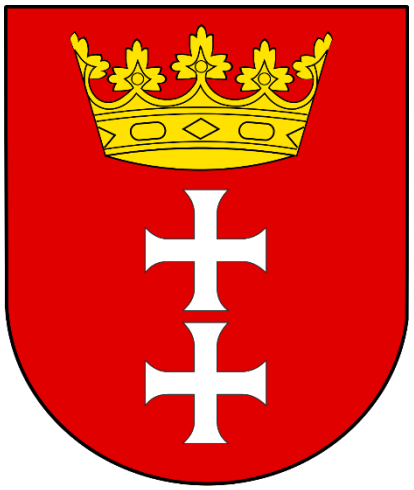
On one hand, in the case of employer-employee situations, freely given consent is rarely ever acceptable for the purposes of data processing. In this case, it appeared that failure to consent to the new system resulted in a personal meeting with the directors. Therefore, employees felt coerced to consent to using the fingerprint scanner.

Moreover, the necessary security reasons which could justify the processing of employee biometric data were inexistent. The authority determined that there were other less invasive options to consider, especially considering that the company's activities did not constitute sufficient grounds for the processing of this kind of data, thus resulting in the processing being highly disproportionate to employee rights and this despite the fact that the data itself was encrypted.

Furthermore, it was reported that whilst the biometric data of ex-employees was inaccessible via the scanner system, it was not permanently deleted and thus was being retained for far too long and without justification.

Going slightly overboard with innovation

March 2020



The city of Gdansk was handed down a fine by the President of the Polish Personal Data Protection Office (UODO) in the amount of €4,600 for unlawful processing of children's biometric data in one of the its local primary schools.

With around 680 students, the school opted for the installation of a fingerprint scanner at the entrance of the school canteen to verify students' pre-payment for their meals. The authority stressed that what was of essence in this case was to consider the necessity of the biometric system to ascertain whether students had paid pre-paid lunches or not. The data being processed here was not only sensitive but also belonged to children, a category of persons whose data requires an even higher threshold of protection. The President of the UODO described the system as disproportionate and inessential to achieving the goal of confirming a child's meal payment.

The UODO also considered that the biometric system was in fact so inessential that an alternative system via the use of an electronic identity card was also in place, for which only 4 students had opted. This system however was significantly unfavourable to the latter, as students not making use of the fingerprint system had to wait at the end of the canteen line until all other students were served.

The UODO President further commented not only on the sensitivity of children's data, but also on the fact that biometric data is not subject to change at any time and is therefore of a unique and permanent nature. This therefore explains the high level of care which must be taken when processing this form of data to adequately protect persons' rights and freedoms.

Data Subject Requests

Parents rule (most times)

March 2020

The Mihou Dimitra Speech & Special Education Centre in Greece was charged with violating a parent's right to accessing his child's personal data following a request being made. The Hellenic Data Protection Authority (HDPA) had initially been involved in the case when the parent filed a complaint when his first access request was refused by the school. The school had denied access as the parent was no longer in a relationship with the child's mother.

Despite the HDPA having ordered the school to follow through with the request after having assessed the circumstances, the school continued to default in this. The HDPA consequently slapped the school with hefty €8,000 fine, with €3,000 given for unjustified failure to comply with the access request, and the remaining €5,000 handed out for failure to act upon instruction from the HDPA.

Whilst the authority recognised the special nature of child's data and the extent to which it must be protected, it also recognised a parent's right to access his or her child's data as their legal guardians. In fact, it pointed out that the only exception to providing such data would apply if the access would result in some danger to the rights and freedom of the child or of other related persons, such as the disclosure of one's location, where such disclosure may pose a threat on the child or any other person. This therefore highlights the necessity of carrying out data protection impact assessments.

As easy as 1, 2, 3. Or maybe not

March 2020

Telefónica Móviles España S.A.U. was handed down a hefty €30,000 fine from the Spanish Data Protection Authority (AEPD) upon infringing its obligations

about a subject access and deletion request made by a customer.

Such requests are multi-faceted in nature and may come in several distinct forms, such as access, portability, correction, or erasure. In the case at hand, a customer of Telefónica had made a request to the company, as the controller of his data, to access and erasure. The individual submitted a complaint before the AEPD, which ordered Telefónica to follow through with the request.

Whilst it appears clear as to which steps the company had to take to fulfil the access request in its entirety, it seems a slight mix-up in action taken resulted in making one of the requests impossible to follow through. Upon a subsequent complaint by the same individual, the AEPD noted that whilst Telefónica had complied with the request for deletion of data, it had previously failed to adhere to the access request. Naturally, following through with the erasure request meant that the request for access could not be fulfilled. Therefore, the AEPD handed down the fine on this basis, also taking into account the fact that the company had failed to adhere with a previous order of the same authority.

Do not bank on it

March 2020

The Croatian Personal Data Protection Agency (AZOP) has issued its first administrative fine, the amount of which is yet to be officially confirmed depending on a number of considerations. Although media coverage of this was largely shrouded by news on the COVID pandemic and the earthquake that recently shook the Croatian capital, the AZOP issued an administrative decision to a Zagreb bank for failure to adhere to customer (subject) requests despite the provisions of specific consumer credit laws.

Over a number of months, the AZOP had received several complaints from customers of the bank regarding access requests in relation to specific loan agreements which were consistently being refused. Upon conducting its investigations, the authority concluded that, over and above the individual complaints made to it, the bank had received around 2,500 requests of this nature between May 2018 and April 2019.

Whilst the bank attempted to argue that the specific credit documentation being requested (which included bookkeeping cards, repayment plans and agreement annexes) did not fall within the remit of the data subject's rights of access, it also argued that the documentation related to loans which had already been repaid and thus the data subjects had no right to request access thereto as per specific consumer credit regulations.

The fine thus came about as a consequence of the bank's failure to adhere to data subject access requests, despite the AZOP having already ordered the bank to comply.

The right to be forgotten & an unforgettable fine

March 2020

In 2017, the Swedish Data Protection Authority (Datainspektionen) conducted an audit into Google's handling of delisting requests from the search engine results for reasons of lack of accuracy or relevance, to name a few.

Whilst back then the authority had ordered Google to act on several counts in this regard, a follow-up investigation in 2018 revealed that the company had failed to comply with the authority's orders. The latter investigation has recently been concluded, resulting in the imposition of a €7 million fine.

The issues that cropped up vis-à-vis the right to be forgotten were twofold. On one hand, a request for delisting of a specific search result had only followed through with a narrow interpretation of what the data subject had requested the removal of. In the second instance, the internet giant had delayed itself in removing a specific result listing without justification.

The Datainspektionen also pointed out that part of Google's delisting procedure was significantly unjust and undermined the fundamental aim of the request at law. Upon adhering to a right to be forgotten request, Google sends a notification to the website whose link is being delisted from the search engine results. This served to prompt the specific website controller, who is then free to publish the information contained in the delisted webpage to another webpage, and Google were therefore ordered to terminate this practice.

Nonetheless, the authority's stance in this regard has been met with certain criticism, wherein it is being argued that website controllers have a right to know that their material is being delisted (at least in terms of the freedom of publication), to allow them the possibility of challenging decisions made in this light.

Short-cut drives company straight into the wall

May 2020

A Danish job recruitment agency, Job Team A/S, has been fined approximately €6,700 for blatant disregard of a data subject's rights and the provisions of the GDPR.

The Danish Data Inspectorate (Datatilsynet) received a complaint concerning the company, wherein upon a subject access request having been made by a data subject, the company proceeded to erase the data required prior to replying that the same data was no longer available.

The Datatilsynet noted that this course of action constituted a categorical denial of the data subject's access rights. In deleting the requested personal data, Job Team (as the data controller) effectively prohibited the data subject from exercising his rights, or at least from attempting to do so. Therefore, the authority noted that the data in question had clearly not been processed in a lawful, fair, and transparent manner, and constituted "a violation of the citizen's fundamental rights".

In this case, the authority not only imposed the relevant fine, but also proceeded with reporting the incident to the police, who shall assess whether appropriate action shall be taken in this regard.

Failure to Inform Data Subjects of their Rights

Information is key

May 2020

Posti Oyj Group, Finland's main postal service provider, was handed down a fine by the Finnish Office of the Data Protection Ombudsman for violating data subject rights in failing to provide them with adequate information on their privacy rights, as guaranteed under the GDPR.

Customers who submitted a change-of-address notification to the service provider had been subjected to several unsolicited direct marketing attempts. The Finnish authority took note of the fact that persons using this notification service were not informed of their right to object to the processing of their personal data for the purposes of direct marketing. However, the option to opt-out was only given to customers who purchased additional services over and above the notification. Informing clients of their right to object to the processing of their data (especially for direct marketing purposes, as in this case) should have been available to all and not simply to specific customers.

Following complaints being made, the Ombudsman had urged Posti to make the necessary arrangements to improve transparency in 2017. The situation was remedied by 2020 by consequence of a follow-up by the authority, in the meantime having affected hundreds of thousands of customers.

Eni plays with fire and burns €11.5 million

January 2020

Two fines running into the millions were meted out by the Italian Supervisory Authority (Garante) for failure to inform data subjects of their rights in two separate cases.

In the first instance, Eni Gas e Luce had blatantly violated its clients' data privacy rights upon their receiving several direct marketing calls, without them having been informed of the option to opt-out from marketing activities. Effectively, several data subjects had even directly objected to receiving promotional marketing calls, yet nonetheless kept receiving them.

It was consequently noted that Eni lacked adequate measures to ensure automated data flow in relation to customers' opt-out requests, which the Garante ordered to be rectified. An order

was also issued to cease the processing of personal data for marketing purposes if specific consent for such reasons had not been obtained beforehand. In conclusion, the Italian energy giant was fined €8.5 million.

On the second count, the Italian Garante became aware that Eni had violated individuals' inherent data privacy rights upon concluding unsolicited contracts for energy supply with the companies with which the data subjects would have been subscribed. Such companies operated as agents to solicit clients for Eni, and both entities would fail to officially inform the circa 7,000 consumers affected of the change. In fact, many of them only realised that the change had occurred upon receiving their first bill under the Eni header.

Several complainants further argued that their data was often incorrectly processed, with others even lamenting that signatures had often been forged in this regard. Therefore, the Italian Garante dealt Eni a further fine of €3 million.

Thank You

First and foremost, we thank, you, the participants, particularly those who had to bear with us until we moved the conference online. This conference was meant to be held on the 27th May, two days after the GDPR's second anniversary, in one of Malta's leading hotels but it was not meant to be. We were not discouraged and understand the importance of this conference. We hope that you enjoyed our online version.

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.

We cannot miss thanking CyberSift for their continuous support for the staging of this conference as well as the Office of the Information and Data Protection Commissioner, the European Commission and 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 😜