fieldfisher

EU Member State Enforcement of the GDPR

Updated: 5 November 2018

Country	GDPR Comments
Austria	GDPR comments: • The Austrian DPA only publishes its decision where the decision has a legal relevance beyond the individual case. As a result, the DPA has so far published only nine decisions since the GDPR became applicable. Furthermore, the publication is always pseudonymous. • Proceedings have commenced in more than 110 administrative prosecutions under the GDPR. In two cases the DPA issued administrative fines. There is no information on the amount of the fine available, since those decisions were not published by the DPA. • There is no information yet about whether the DPA performed audits or investigations into specific organisations or industry sectors. Due to the current number of employees, the DPA is only able to handle day to day operations. Therefore, it is assumed that such audits or investigations are not planned for the near future. • **Since May 25th, more than 750 complaints were filed with the DPA. The majority of these complaints are cross-border cases and therefore the DPA had to inform and involve a partner agency in another country, or was informed by a partner agency.** • **The DPA registered more than 250 data breach notifications. Most of these cases were ceased and the DPA did not investigate further. In two cases, the DPA requested a controller to inform data subjects pursuant to Article 34 of the GDPR, via the enforcement notice. One case in particular involved the loss of a book which held sensitive data about patients who were addicted to drugs.**
Belgium	GDPR comments: • **On average 4 data breaches per day are reported to the DPA. Depending on the severity of the data breach that is reported, the DPA may ask for clarification and additional information on e.g. the circumstances of the breach, the actions that were already undertaken etc.** • **None of Your Business reported it filed a complaint to the DPA on 25 May against Facebook Ireland Ltd. in relation to Instagram. We do not know what the status of this complaint/investigation is.** • We are not aware of any other enforcement actions with respect to the GDPR in Belgium.

	Non-GDPR comments: • In a judgement of 16 February 2018 following a legal battle between the Belgian DPA and Facebook which started in 2014, the Court of First Instance of Brussels has convicted Facebook for non-compliance with the Belgian privacy and cookie rules. The Court ordered Facebook to cease its current cookie use practices under forfeiture of an incremental penalty of 250 thousand EUR per calendar day of non-compliance (with a maximum of 100 million EUR). Facebook is expected to appeal this decision.
Bulgaria	GDPR comments: • The Personal Data Protection Amendment and Supplement Act (PDP ASA) to set the national legislation in compliance with GDPR is expected to be adopted and entry into force within the next two months at the latest. • The Bulgarian Commission for Personal Data Protection (CPDP) has adopted Guidelines on Preparation and Application of Codes of Conduct pursuant to article 40 of the GDPR, Criteria and Procedure for Approval, Amendments and Supplements of Codes of Conduct as well as Guidelines on the Personal Data Processing Consent. • CPDP has further adopted six opinions on GDPR application of based on requests of controllers from the public and private sectors regarding publishing of personal data for media purposes, notions of 'controller' and 'processor', using one consent for direct marketing by joint controllers and voice biometrics. • **At the time GDPR entered into force the Chairman of the CPDP announced that when CPDP establishes violation of the GDPR, CPDP will first issue reprimands and afterwards will impose sanctions.** The statement is in compliance with the PDP ASA, which in fact resembles the now applicable national piece of legislation – CPDP is indeed entitled do issue reprimands as a first step towards compliance with personal data regulation. Of course, this would not go for any material breach of legislation. • Since GDPR entry into force CPDP has not imposed sanctions under these legislative rules yet. In may be because of the approach that the CPDP will take (i.e. to first issue a reprimand); but it may also be due to the fact that the PDP ASA is yet neither adopted nor effective. • **Within the period May-October 2018 CPDP issued one decision which reprimanded a controller (i.e., the National Directorate Construction Control (ДНСК)) for violation of the current Personal Data Protection Act as well as two orders with relation to the application of the GDPR.** Non-GDPR Comments: • I**n several appeal decisions Supreme Administrative Court has only commented on the application of the GDPR. No sanctions imposed.**
Croatia	• The activity of the Croatian supervisory authority (AZOP) is not made public so information about enforcement activity is not publically

	available.
Cyprus	• The Commissioner has announced **compliance audits to take place starting from September 2018.** • **There have been no public announcements on any enforcement actions taken as of yet.**

Czech Republic	GDPR comments:
	• A number of companies were fined for sending commercial communication and for email marketing –
	  ○ EC PROFIT:CZK 800,000/approx. EUR 30,951.10 (June 2018),
	  ○ SOLIDIS: CZK 800,000/approx. EUR 30,951.10 (August 2018) and
	  ○ Kelpias Consulting (CZK 86,000/approx. EUR 3,327.25).
	• The Office for Personal Data Protection (Office) points out that it continues to pay close attention to the malpractice of using some third-party databases for the distribution of commercial communication.
	• In October 2018, the Office (the DPA) imposed a fine of CZK 1.5 million (approx. EUR 58,033.40) on Internet Mall, a.s., one of the Czech largest e-shops.. The reason was that the company did not provide sufficient security guarantees for personal data of at least 735 thousand customers, which resulted in a personal data breach (please note the breach occurred and the proceeding commenced before GDPR).
	• In the CERD (Central Debt Registry – privately operated database) investigation, **the Office imposed corrective measures aimed at removing the errors detected in the CERD system**. **The DPA´s representative Mr Jiří Žůrek encouraged the data controllers that it is not the DPA´s goal to impose the highest possible sanctions, but rather to ensure rectification and to strengthen awareness about personal data protection.**
	• One of the new cases investigated by the DPA is the announcement of a data breach committed by a building society. The DPA was reported a client's data breach, which was due to the erroneous electronic dispatch of personal data of more than 300 people to 147 different addresses.
	• A man who found a USB flash drive containing contracts including personal data in one of the department stores in the Central Bohemian region contacted the DPA. The DPA will therefore focus on whether the controller breached the GDPR by not implementing adequate technical and organizational measures to ensure the security of personal data.
	• Several times the Office has been addressed by doctors who believe that the operator of the www.znamylekar.cz portal processes personal data besides the commonly available personal data about the doctors in a way that is in contrary to the rules regarding protection of privacy and personal data. **As the processing of personal data on the portal www.znamylekar.cz is carried out by Polish company, the competent**

	Polish data protection authority will now cooperate with the Czech Office on this matter in accordance with the established mechanism. The Office will subsequently inform the public about the outcomes of the investigation.

Denmark	GDPR comments:
	• **As of 5 October 2018 the Danish Data Protection Authority (DDPA) has received around 1,500 data breach notifications since 25 May 2018, corresponding to about 83 notifications per week.**
	• One Danish municipality has reported 35 notifications of data breaches since the 25 May 2018.
	• One of the larger data breaches reported to the DDPA was made by a television provider, Stofa. A hacker gained access to more than 2,000 customers' usernames and personal passwords.
	• Examples of the breach notifications that the DDPA has received are:
	  ○ National identification numbers were made available through regular citizens access to a public system;
	  ○ A national identification number was not anonymised in a request of access;
	  ○ Emails were forwarded with personal information including name and national identification numbers;
	  ○ Website showed unauthorised citizens' name, address, national identification numbers and grade point average;
	  ○ Summary disclosed a citizen's protected address.
	• There are **ongoing inspections regarding the designation of a DPO** at private hospitals and public health institutions.
	• The DDPA also has **ongoing inspections regarding the legal bases for processing personal data and risk assessments** with both a Danish dating website and a larger Danish beauty chain.
	• The DDPA has **ongoing inspection regarding erasure of personal** data with a larger hotel chain
	• The DDPA has published **the compliance issues of their planned inspections until the end of 2018**, which will focus on:
	  ○ The legal bases for processing personal data and risk assessments in private companies
	  ○ Erasure of personal data in private companies
	  ○ Use of data processors with the municipalities
	  ○ Security for personal data in larger IT systems within the health care area
	  ○ Designation of DPO – public authority and private companies
	  ○ Drawing up of records of processing activities with municipalities
	  ○ Rights of the data subject after the Law Enforcement Act

	○ Data processing activities in relation to EU-information systems, e.g. Schengen Information System (SIS) • The DDPA has released examples of the questionnaires they are using during their inspections • The DDPA expects that the **first fines will be issued during late fall or around Christmas 2018** • **The security breach at Facebook, which compromised about 50 million profiles is followed closely by the DDPA. They are working with the other European Supervisory Authorities regarding the case.** The DDPA has changed the practise when receiving a notification of a data breach. Before investigating a data breach the DDPA informs that the case might lead to criminal persecution and that the controller is not obligated to provide any further statements.
Estonia	GDPR comments: • Estonian data protection authority (DPA) has not yet issued sanctions under GDPR. • **DPA has stated that it will have a closer look at processing of employees' data and also personal data processing by local authorities. The DPA will also audit companies' chain of command to test the response in the event of a data breach.** • **The DPA received 33 breach notifications** within the first 3 months since the GDPR has applied (approximately 2 per week). 17 of them were notifications regarding hacking, 4 were security loopholes and other different faults of the controller/processor. • There have not been any notifications regarding more severe breaches. • The DPA's call line has received a higher volume of requests for information and the DPA now publishes different guidelines explaining the GDPR. • There is no information yet about fines issued under the GDPR but note that local law has not yet been amended to allow GDPR level fines. • **The Estonian DPA has been involved in several international proceedings**. • Cyber breaches and attacks are also monitored by the Estonian Information System Authority. In August 281 they registered 218 incidents. They also dealt with the cases where GP's systems were attacked with ransomware.
Finland	GDPR comments: • The Finnish SA, the Data Protection Ombudsman, has not yet been active on GDPR related issues. • Currently, information regarding fines issued or threated to be issued by the Finnish DPA is not publicly available. Furthermore, **the Data Protection Ombudsman does not yet have the powers to issue fines, as the local Data Protection Law has not yet been enforced.** At the

	moment of writing, it is unclear when the law will be enforced. Enforcement notices and information regarding data breaches are also not publicly available. • **The Ombudsman states that audits will only now start in Finland (from 12 October). The Ombudsman also states that some companies under investigation in Finland are the same companies as in Sweden, including network operators Tele 2 and Telia, and financial operators Forex Bank and Resurs Bank.** • **The Ombudsman also states that they have received 300 notifications of cross border related breaches. It has also been reported that cross border cooperation has been very active, and that the DPA had received dozens of contacts from other member states.** • It has been noted that activity has generally increased substantially. The Ombudsman has received 1,300 notifications concerning data protection violations and approximately 300 national complaints.

France	GDPR comments:
	• **It is important to note that the DPA's proceedings are generally not public. Therefore we may not be aware of some on-going investigations and actions. Nevertheless, more than 600 notifications of data breaches have been received by the French DPA involving about 15 million people - about 7 per day since May 25.**
	• Since May 25, **the CNIL has received 3767 complaints** against 2294 complaints over the same period in 2017. This represents a **64% increase**.
	• **The CNIL entered two orders against the startups "Fidzup", "Teemo" and "Singlespot" to cease and desist from violating the French Data Protection Act and the GDPR (especially on the legal basis/consent ground). These companies use location data for advertising targeting purposes through a technology installed in mobile applications. Teemo complied with such regulations and the proceeding has been closed on October 3rd 2018. We are still waiting for the Fidzup and Singlespot decisions.**
	• **The CNIL entered an order against a private university, the "Institut des techniques informatiques et commerciales (ITIC)" to cease to permanently film staff, teachers and students on the premises and to comply with various GDPR provisions. It reminds ITIC that the Commission considers excessive any CCTV system that places employees or students under constant surveillance.**
	• As regards to joint-actions, two organizations have filed complaints with the CNIL
	  ○ "La Quadrature du Net" filed 5 separate complaints over "forced consent" against Google, Amazon, Facebook, LinkedIn and Apple.
	  ○ The association "NOYB" filed a complaint over “forced consent” against Google (Android).
	• As part of the cooperation between supervisory authorities the CNIL will hear complaints concerning the conditions under which the Belgium NGO "EU DisinfoLab" carried out a study on certain messages published on Twitter relating to the Benalla affair. This study especially

	focused on the impact of the Benalla affair on social networks and reveals users' supposed political affiliation. The Benalla affair is a political and judicial case involving Alexandre Benalla, who served as a security officer and deputy chief of staff to French President Emmanuel Macron. In June, he was identified in footage as the person who beat up a protester during the 2018 May Day demonstrations in Paris. Preliminary investigation where opened for violence and concealment of image from a video surveillance system. Parts of the French political class questioned the Élysée's responsibility in the case for its apparent concealment of the case from the public prosecutor. • **To our knowledge, no companies were fined under the GDPR yet.** Non-GDPR comments: • The French company "Optical center" has been **fined EUR 250,000** by the CNIL for failing to secure its website. It was possible to access hundreds of customer invoices, containing health data and, in some cases, the social security number of the data subjects concerned. This case is one of the **highest sanctions ever pronounced by the CNIL before the GDPR came into force and illustrate the seriousness by which the French DPA is taking data protection.**
Germany	• **It is unlikely that any sanctions have already been imposed under GDPR in Germany yet. Marit Hansen from the data protection authority in Schleswig-Holstein laid out that in short cases six months for the issuing of the first GDPR fines** would be quick. For other cases (the majority) it would take longer. This is comparable with state prosecutions where in Germany a case may take more than a year, according to Hansen. • **According to a ministerial decision of the Bavarian State Government, data protection authorities should act "appropriately and with a sense of proportion" in the enforcement of the provisions of GDPR against small and medium-sized companies and volunteer associations. This includes not imposing fines for first-time violations of the GDPR. It is however questionable whether this modest application of the GDPR and in particular the renouncement of fines for first-time violations is GDPR-compliant.** • The Bavarian State Authority for data protection announced **random controls of companies from September 2018.** • During the months May-July 2018, the Data Protection Commissioner of Berlin received 1380 data protection complaints by citizens. In the same period in 2017 the authority only received 344 such complaints. • During the months May-July 2018, 111 data breach notifications were filed with the Data Protection Commissioner of Berlin. In the same period in 2017 the authority only received 12 of those notifications. • **Three months after the GDPR entered into force, the Data Protection Commissioner of Berlin has not yet imposed any sanctions. According to this authority a sanction procedure takes some time to complete due to the strict procedural rules.** • The Bavarian data protection authority forbids the use of the marketing tool Facebook Custom Audiences without consent of the data

	subject, as it is considered to be incompatible with GDPR-rules. The administrative court Bayreuth confirmed this decision in summary proceedings. • **The Lower Saxony Data Protection Commissioner has sent GDPR questionnaires to 50 companies (30 of them larger and 20 mid-sized) from various industries with headquarters in the federal state in September 2018: Data protection authorities carry out random checks, first fine proceedings underway.** • Under German competition law, it is possible for companies and individuals to obtain injunctions against competitors in the event of infringements of the law. It is controversial whether a breach of data protection law is sufficient for this. The state court in Würzburg has recently issued a temporary injunction for an infringement of Art. 13 GDPR. Following this decision companies and individuals obtain the factual power to enforce compliance with the GDPR, but we await clarification on this issue by the Federal Court of Justice.
Greece	• The Greek Authorities are slow to implementing the GDPR. For instance, the national GDPR implementation law of the GDPR is yet to be enacted, although the relevant consultation was concluded since last March. • **We are not aware of any enforcement actions under the GDPR but this should definitely not be interpreted as a lack of seriousness or interest in data protection, but rather it reflects certain bureaucratic inefficiencies of the Greek public sector.**
Hungary	GDPR comments: • **To the best of our knowledge no fines have yet been issued by the DPA under the GDPR nor are we aware of any investigations into specific organisations or industry sectors, but audits will take place soon.** • **The SA is generally quite active and be likely be coordinating its actions with SAs in other countries.** • Information about enforcement notices under the GDPR is available on the SA's website. • Historically the SA has taken a strict approach to data protection compliance and the same trend is expected under the GDPR although we are aware that the SA have had serious workforce problems which is partly due to the current high need for privacy experts. Non-GDPR comments: • Pre-GDPR, the Hungarian SA twice imposed a fine amounting to HUF 20 million (approx. EUR 62,000, being the maximum fine under the Hungarian Act implementing the Directive) on the Hungarian Church of Scientology for various serious breaches of the local Data Protection Act.
Ireland	GDPR comments:

	• **The SA has commenced an investigation into the Facebook data breach, notified to the DPC on 28 September.** • **An investigation has commenced into Google's use of location data.** • The SA has dealt with a high-profile data breach of Eir customers' data. DPC expressed concerns about technical and structural security measures of organisations. • **The DPC received 1,184 reported data breaches in the first two months GDPR was in force, compared with the average of 230 reported each month in 2017. GDPR applies in 953 cases.** • Up to July 2018, the DPC received 514 DPO notifications across a wide range of public and private sector organisations. • Up to July 2018, the DPC has more than 100 "one-stop shop" cases registered in its system (37% assume Ireland is the lead supervisory authority, 13 % Germany and 11% Luxembourg). Non-GDPR comments: • The DPC has received additional funding of €3.5m in the 2018 budget, bringing the total funding to €15.2m
Italy	GDPR comments: • Ongoing investigation on the platform called "Rousseau" of a political party to check for any new data breach. • **The Italian DPA received 305 breach notifications and 2,547 complaints and reports (compared to 1,795 in the same period of 2017) in in the last four months.** • **In the context of the "Privacy Sweep 2018", the Italian DPA stated that its action will be concentrated on the Regions and the Autonomous Provinces and on the respective subsidiaries that carry out relevant processing of personal data for the performance of tasks of public interest.** • **In the period from January to June 2018, the inspection activities carried out by the Italian DPA, also by the Financial Police, has been directed to: *a)* the processing of health data carried out by Local Health Authorities ("ASL") in relation to the transfer of health data to third countries for scientific research purposes; processing carried out by statistical information systems (e.g., ISTAT); processing of personal data carried out by companies for telemarketing activities; data processing carried out by companies for rating activities on the risk and solvency of companies; *b)* to verify the adoption of security measures by individuals, public and private, who carry out processing of sensitive data.** • **In the period from July to December 2018, the inspection activities carried out by the Italian DPA, also by the Financial Police, will be directed to data processing carried out by companies / entities that manage large databases; processing of personal data carried out with**

	credit institutions regarding the legitimacy of consultation and subsequent use of data, also with reference to the tracing of accesses and related security measures; processing of personal data carried out by companies for telemarketing activities; • The Italian DPA will carry out the most appropriate initiatives with reference to the secret agreement between Google (Alphabet) and Mastercard to track "offline" purchases of US consumers for advertising purposes, also in cooperation with the other the European Supervisory Authorities. Non-GDPR comments: Whilst not awarded under the GDPR the following fines indicate the level of fines that companies may be subject to • In May 2018, Telecom were fined EUR 960,000 for: (i) the unjustified assignment of a large number of telephone users to a single person, due to unspecified errors occurring during the migration of customer data from a management system between 2002 and 2004 (EUR 800,000); (ii) a data breach case at the end of 2013 that revealed customers' data (EUR 160,000). • Several companies were fined for marketing activities: Fastweb (EUR 600,000: July 2018); Vodafone (EUR 800,000: July 2018); Wind Tre (EUR 600,000: May 2018).
Latvia	GDPR comments: • **The Latvian SA is not very active yet (although there are several cases underway).** The details will be disclosed once an official decision has been made. Additionally, the SA does not report publicly on individual fines levied. According to publicly available information the approximate planned budget for data protection fines is EUR 200,000 for 2019 and EUR 500,000 annually thereafter. • According to official statistics, 70% of the workload of the SA is consultations. The local laws on administrative penalties are being updated, as a result, the Latvian SA is meant to base fines on the GDPR. The result is yet to be seen in practice, but the gap between the previous cap of EUR 14 000 and EUR 20M is considerable. Moreover, the SA investigation and decision-making process usually takes at least 6 months. Non-GDPR comments: • **The biggest pre-GDPR fine was EUR 11,400 (with the maximum applicable 14 000 EUR according to the previous law)** for publishing the personal data for commercial purposes on Facebook and Twitter. The fine was imposed on a legal entity. However, there are no fines issued yet under the GDPR. • There is another Latvian SA charged with fighting corruption (the Corruption Prevention and Combating Bureau (KNAB)). KNAB imposes fines for unlawful access to personal data by state officials and employees of authorities. However, these fines are not based on the GDPR. There have been a range of criminal cases related to the same access issue.
Lithuania	GDPR comments:

	• **The SA has generally taken a gentle approach to the GDPR, so not enforcement activities have yet known despite over 150 written complaints after the 25 May, 2018. The SA has only issued recommendations and corrective measures. The investigated companies now have up to two months to correct the ill practices or face a fine.** • **SA has initiated an investigation of 12 entities working in pharmacy, home appliances and food sectors. All of these entities were chosen because they have loyalty programs and perform direct marketing. Various breaches have been identified in all of the investigated companies.** The breached were related to lack of transparency, scope of processed personal data (excessive data was processed), failure to provide initial information about processing activities, term of data storage (in most cases it was indefinite or too long (10 years, throughout the lifetime of the company)). • **In banking sector there is a verbal agreement between the SA and the banks that currently the banks will notify every data breach, regardless of the impact. The idea is that SA now closely monitors what types of breaches are most common.** • **The other sector which undergoes planed inspections by the SA this year is gardener's communities. It is a sector which is almost completely unprepared for the GDPR.** • The other institution which is responsible for the electronic communications, namely Communications Regulatory Authority, is rather passive. • Until now, there are about 685 notifications about appointed DPO's. Which is relatively low and only 134 of DPO's have been appointed in public institutions.
Luxembourg	<u>GDPR comments:</u> • On 28 September 2018 the SA reported that: there has been 97 data breaches notified to the SA between 25 May and 27 September 2018. 36% of the data breaches are external malicious acts and 56% are internal accidents. Around 20% of the data breaches are considered to have a significant potential impact for the data subjects. • **Regarding enforcement actions in application of the GDPR (fines issued or threatened, enforcement notices) we are not aware of any such actions taken by the Luxembourg SA yet and there is no publicly available information on that issue. It should be noted that the law implementing the GDPR and granting enforcement powers to the Luxembourg SA is dated 1 August 2018 and is applicable since 20 August 2018. Before that date, the Luxembourg SA was not entitled to take enforcement actions in application of the GDPR. It is therefore too early to assess enforcement actions under the GDPR.**
Malta	• **To date, the SA has published very little information about investigations or actions taken. Such information would only become public if/when a decision of the IDPC is actually appealed (before the Administrative Tribunal and eventually at Appeal Stage). In our opinion it is**

	still premature for any such decisions taken post 25th May to have become public in this manner. • **The IDPC has disclosed that up to the 2nd October 2018, the SA issued 8 data protection complaints decisions in terms of the GDPR and 34 data breach notification decisions.** No decisions included an administrative fine pursuant to the GDPR. The details are not public and therefore we cannot comment on their merits.
Netherlands	GDPR comments: • The Dutch DPA collected an incremental penalty of € 48,000.-- from TGB, a private bank in the Netherlands, for repeatedly not complying with a SAR. • The Dutch DPA found that the practice of the tax authorities regarding the usage of VAT registration numbers does not comply with the Dutch GDPR Implementation Act and leads to unnecessary privacy risks. The tax authorities issue VAT registration numbers for self-employed workers without employees. However, this VAT registration number is to a large extent the same number as the citizen service number of the relevant self-employed worker without employees. This practice does not comply with article 46 of the Dutch GDPR Implementation Act which states that a number that is required by law for the identification of a person, can only be processed for the purposes provided by the law. The Dutch DPA did not stipulate which measure should be taken to end the breach. The tax authorities assured the Dutch DPA that a plan of action would be presented before summer 2018. However, until now no plan of action has been presented by the tax authorities. Most likely we will hear more about this particular case in the near future. • **On the 17th of July, just after the GDPR came into force, the Dutch DPA started an arbitrary (random) investigation into thirty large organisations from ten private sectors in the Netherlands to review if they keep records of processing activities. The following industries were examined:** ○ **Industry** and **metal;** ○ **Water company;** ○ **Construction;** ○ **Commerce;** ○ **Catering industry;** ○ **Tour operators;** ○ **Communication;** ○ **Financial services;** ○ **Business services;** ○ **Healthcare;** **The chairman of the Dutch DPA announced in a radio-interview on the 17th of September that the DPA imposed an order for incremental penalty payments (*last onder dwangsom*) for non-compliance of some of these companies. The chairman did not disclose**

	which companies. • **The Dutch DPA checked 91 hospitals and 33 healthcare insurers in order to assess whether they appointed a DPO. This investigation showed that 25 % of this sector was not compliant. The DPA decided not take enforcement actions, but gave the respective parties merely a warning and a (new) chance to comply with the GDPR.** • On the 29th of June the Dutch DPA published a statement in which it stated as of 25 May 2018, more than 600 complaints were filed with the DPA. Of these complaints, 87% were about businesses and the other 13% about government agencies. At the time of publication of the public statement, the Dutch DPA had analysed 400 of the 600 complaints, of which 1/3 dealt with the unwillingness of companies to honour the right to be forgotten/right to the removal data and the difficulties data subjects encountered in exercising this right, 18% of the complaints were related to the disclosure of personal data to third parties and 5 % of the complaints touched upon SAR's. 84 of the 400 analysed complaints were cross-border complaints. Non-GDPR comments: • The National Police needs to protect the police data in a better way. In 2015, the Dutch DPA imposed an order subject to a penalty of €200,000.—to resolve 5 vulnerabilities. The police only resolved 4 out of 5 vulnerabilities, therefore the incremental penalty was of €40,000.—was collected. The fifth measure was to control the log files in a regular and proactive manner. At the moment, the Dutch DPA are re-evaluating if the police is compliant regarding to this matter.
Poland	GDPR comments: • For the first three months following 25 May 2018 the Personal Data Protection Office (Polish DPA) received about 2,400 complaints of the data subjects compared with 3,000 received by the Polish DPA (former: Inspector General for the Protection of Personal Data) in 2017. Majority of these complaints related to the breach of Art. 13 GDPR (obligation of information to be provided where personal data are collected from the data subject), breach of the right to erasure (Art. 17 GDPR), illegal processing of personal data for marketing purposes or spamming; • For the first 3 weeks of GDPR being in force, Personal Data Protection Office (Polish DPA) received 150 complaints from the data subjects and about 150 data breach notifications from the data controllers. DPA also received a lot of questions from the data controllers relating to the application of GDPR. Most of these questions concerned monitoring, there were also questions from the hospitals relating to the access right to the medical documentation; • **Polish DPA initiated ex officio an investigation relating to creating the so-called "black lists of patients", i.e. an Internet portal which makes available to doctors an non-anonymized lists of patients which are notoriously late or never keep the medical appointments;** • **Due to the new regulation introduced to Labour Code regarding CCTV in the workplace, President of the Office announced an adjustment**

	period (which lasted until the end of September) when the entities were not punished for non-compliance with GDPR in the field of monitoring; • In connection with personal data breaches on Facebook, the President of the Office has cooperated on the base of procedures provided by GDPR with the Irish data protection authority and other data protection authorities to determine the scale of the breach; • As the above mentioned breach notified by Facebook included the personal data of Polish users, Polish DPA also joined the proceedings conducted by the Irish data protection authority regarding personal data breaches on Facebook mentioned above. • **Currently no published reports regarding fines or threatened fines imposed by the Polish DPA.**
Portugal	GDPR comments: • The Data Protection Act that will implement the GDPR in Portugal and approve any derogations has not been approved yet. Instead the Supervisory Authority has been issuing some guidance and developing means for DPO and data breach notification purposes. • On October 11 the Portuguese Supervisory Authority **issued fines totaling EUR 400,000 to a hospital in Portugal** for breaching the minimization and confidentiality principles and not being able to ensure such principles (e.g. unauthorized access, no access rules, authentication flaws, no separation of health data and administrative data). • **There are no (at least public) records of any other fines issued or threatened, audits undertaken, investigations, enforcement notices.** • **The Supervisory Authority has not yet made public the number of data breaches notifications received or of DPOs appointed so far.** • Regarding Facebook, the Portuguese Supervisory Authority has just made a statement to the media that will follow closely the procedures and investigation of the British and Irish Supervisory Authorities in this regard. • Concerning complaints presented so far, the Supervisory Authority has also declared that the number of complaints is low when compared with other countries. • The annual report regarding 2017 has not been published yet. • **The activities plan for 2018 states, as far as enforcement is concerned, that audits and inspections will occur where necessary and that investigations procedures will be developed by means of check lists to facilitate the investigators' work field.**
Romania	GDPR comments • **The Romanian Supervisory Authority has initiated a series of investigations both ex officio and following the filing of a significant number**

	of complaints and referrals. • **The Romanian Supervisory Authority received about 100 breach notifications since the GDPR became applicable. In most cases, the Supervisory Authority has initiated written investigations, requesting additional information from data controllers. In approximately 15% cases, the investigations were completed without sanctions.** • Starting May 25, 2018 the Supervisory Authority received a total of approximately 1,700 complaints and referrals, which represents a significant increase compared to 2017. • **Until now, from what is publicly known, no sanctions have been applied under GDPR by the Romanian Supervisory Authority**.
Slovakia	GDPR comments • **The Slovak DPA issued a plan to audit certain public organisations in 2018**, including: municipalities, EUROPOL, EURODAC, SIRENE and Slovak consulates. The DPA does not plan to control private organisations from its own initiative in 2018. • The DPA has developed an online form for data breach reporting available here. • According to published information the DPA will not hesitate to enforce the regulation and impose high fines, however to the best of our knowledge there have **not been any significant fines in issued since the GDPR is applicable**. • Please note that throughout the year the DPA does not publish information about breach notifications, nor about fines or actions taken. The DPA publishes a yearly report on data protection in Slovakia. The reports are available here. • Please also note there have been no reports or news on data breaches in Slovakia so far.
Slovenia	• To date, there is no concrete information or reports on the open procedures, fines, potential sectoral inquiries etc. in any publicly available sources, or the media. • The Slovenian Information Commissioner ("IC") is (or more accurately, will be) the competent regulator and enforcement authority for the GDPR in Slovenia. • **Due to the fact that the Slovenian implementing act has not been adopted yet (the amended Data Protection Act ("ZVOP-2") is currently still in the legislative procedure and still has to be voted on by the Slovenian Parliament), the IC is somewhat limited in regard to its powers for imposing fines.** At the moment, the IC can only impose fines for breach of the still applicable provisions of the currently valid Data Protection Act ("ZVOP-1"), which means that it cannot impose fines for any potential breach of the GDPR and / or any potential breach of the provisions of ZVOP-1 which were derogated by the GDPR. This is also the standpoint and the interpretation of the situation as put forward by the Slovenian Ministry of Justice.

	• This does not affect the performance of subjects and does not hinder the commencement of potential offence proceedings, if the breach concerns the applicable provisions of ZVOP-1. All other offence proceedings are suspended until the adoption of ZVOP-2. • **Currently no information on any cases of data breach reported, patterns of data breaches detected or joint actions performed/intended**.

Spain	The Spanish SA does not publish all of its decisions. At the moment, access to decisions is limited because the Spanish DPA is migrating its' website. The Spanish DPA has been very active in issuing guidance and setting out schemes in collaboration with other bodies with the aim to promote GDPR compliance, below is a snapshot of this activity. Please also note that the Spanish law which will complement the GDPR is not in place yet.
	
	Regulation:
	• The Royal Decree-Law 5/2018, seeks to put in place a number of rules / procedures in order to provisionally adapt the Spanish data protection legislation to the GDPR in the absence of a new data protection law, which is currently in draft. The scope of the Royal Decree is very limited and it deals with formal and procedural matters such as appointing the Spanish data protection authority as the representative for Spain before the European Data Protection Board (EDBP) or setting out limitation periods for breaches of the GDPR.
	GDPR comments:
	• The Spanish SA has issued guidance documents (Guides) on a variety of topics, including the use of video cameras for security and other purposes; the management and notification of security breaches; DPIAs and risk assessments.
	• The SA's documents and reports includes:
	  ○ Data protection and crime prevention
	  ○ Record of processing activities
	  ○ DPIA checklist
	  ○ Internet privacy policies
	  ○ Decalogue of the most relevant aspects that must be taken into account by those responsible to comply with the GDPR.
	• Voluntary mediation system developed between the Spanish Agency for Data Protection (AEPD) and the Association for Self-Regulation of Commercial Communication (AUTOCONTROL).
	• SA's online platform ("Sede Electrónica") created in order to lodge complaints; DPO registration; etc.
	• SA's creation of FACILITA, a free assessment tool for any company or professional to assess (not for high risk processing).

	• On 19 July 2018, 4 out of 10 SMEs didn't know about the new GDPR regulation. A survey made by SA and CEPYME highlighted that the most frequent processing activiites of SMEs about processing personal data are those of clients, suppliers and employees (90%) and, to a lesser extent, those related to video surveillance (38%) and online forms (17%). • SA and Spanish Compliance Association (ASCOM) have signed a General Collaboration Protocol to promote the DPO role amongst others. • 35% increase in registrations to the do-not-contact list since the application of the GDPR. Non-GDPR comments: • Despite not based on GDPR, the FACUA consumer association has denounced Facebook for an alleged violation of the data protection rights of consumers, considering that the social network procedure differs from what is included in the Spanish Data Protection Law which transposed the Data Protection Directive. • Between 2016 and 2017 there has been an increase of +36.8% of complaints filed through the Spanish Data Protection Agency (AEPD) in relation to the processing of data on Internet, from 557 in 2015 to 762 in 2017.
Sweden	GDPR comments: • The SA has received a total of 1301 reported data breach notifications up to 8 October 2018. • According to the SA, there are no special trends in reported data breaches except that the general level of when a breach is reported seems to have been lowered. • **The SA currently has started a total of 76 audits of which none have been completed. Five initialized audits has been closed due to wrongful registration.** • **No fines have been applied as of 9 October 2018.** • High profile reported incidents include a joint incident reported by the Swedish taxation office and the telecom provider Telenor. • **The Swedish SA has an ongoing investigation regarding compliance with appointing a DPO**. The first investigation, started in June 2018, focuses on regulatory authorities, private caregivers, communal transport, labor unions, telephone operators, insurance companies and banks. • Although initialized previously to the Directive, DI is continuing its investigation on Google and its compliance with "the right to be forgotten". The investigation is now being conducted under the GDPR with the new authority granted DI under the GDPR.

United Kingdom	GDPR comments: • First GDPR Enforcement notice issued against AIQ to cease processing personal data in relation to data analytics, political campaigning or advertising. • Ongoing investigation and audits into political parties, universities and data brokers in relation to data analytics for political purposes. • The Information Commissioner's Office (ICO) received 1792 breach notifications in June 2018, compared with 367 in April 2018. • There have been a number of high profile breaches for which fines are possible such as British Airways, the Conservative Party, and Facebook. • The ICO has begun formal enforcement action against 34 organisations that have failed to pay the new data protection fee. Those who don't pay could face a maximum fine of £4,350. • A number of companies were fined (under the Privacy and Electronic Communications Regulations) for sending emails seeking consent for email marketing - Honda (£13,000) and Flybe (£70,000). Given the higher standard for consent under the GDPR, organisations need to carefully consider their direct marketing strategy. Non-GDPR comments: • Supermarket chain Tesco has been fined £16.4 million by the Financial Conduct Authority for failing to exercise due skill, care and diligence in protecting customers against a cyber-attack. Whilst not awarded under the GDPR it indicates the level of fines that companies may be subject to and confirms in very clear terms that the age of the big data protection fines has arrived. • Although issued under the Directive, the ICO for the first time issued its maximum fine of £500,000 against Equifax for its security breach indicating that the ICO is gearing up for higher fines in the future.