November 2019

In this issue:

The Privacist - Volume 2

A monthly round-up of data protection and privacy developments across the world.

By Natali Adison, Claude-Étienne Armingaud, Eleonora Curreri, Alessandra Feller, Jeremy McLaughlin, Thomas Nietsch, Linda Odom, John ReVeal, Judith Rinearson, Lucile Rolinet

EU: IAPP Europe Data Protection Congress 2019 and Paris Pre-congress KnowledgeNet Meeting

- November will see several opportunities to discuss privacy matters in Europe and meet with *The Privacist* contributors within the K&L Gates' platform, in connection with the International Association of Privacy Professionals ("IAPP").
- On 18 November 2019, K&L Gates Paris will be hosting an IAPP KnowledgeNet focusing on compliance audit procedures. Speakers will include a representative from the Conformity Department of the French Supervisory Authority (Commission Nationale de l'Informatique et des Libertés or "CNIL"), Elisabeth Fraikin (Group DPO, Ariane Group), Matthieu Camus (Privacy Impact), Damien Chaminade (Internal Audit Director), and Lucile Rolinet (Associate, K&L Gates). You can register for the free event here.
- Between 18 and 21 November, the IAPP Europe Data Protection Congress 2019 will take place in Brussels. K&L Gates Brussels' Natali Addison, as well as K&L Gates Paris Claude-Étienne Armingaud and Etienne Drouard will be delighted to meet with you if you are planning to attend!

EU: Publication of new draft of ePrivacy Regulation

- On 4 October 2019, the Council of the European Union released a new proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC ("ePrivacy Regulation").
- Coming a few days after the CJEU's Planet49 decision, this new draft explicitly require that "consent" required for cookies must be construed as a freely given, specific, informed, and unambiguous GDPR consent, while also allowing for consent to be obtained by "appropriate" technical settings of software.
- End-users will need to be reminded of the possibility to withdraw their consent to processing of electronic communications content or metadata at least once per year, unless they request not to receive such reminders. This does not apply to consent for cookies or direct marketing by email or SMS.
- The issue of cookie walls, where access to a service is conditioned to the consent for cookies used for advertising purposes, has been heavily amended. The reference to the end-users "*accept*[ing] *such use*" after being provided with "*clear, precise and user-friendly information about the purposes of the cookies or similar techniques*" could infer a distinction with the GDPR-based consent detailed above and confirm that the debate is far from being closed.

The Privacist - Volume 2

- Direct marketing operations through email or SMS for a company's own products and services to existing customers would remain based on legitimate interest with a right to opt-out to be presented not only in each communication but also upon the initial collection. The new draft offers Member States the possibility to set an expiration time on such use, after which opt-in consent may be required. Such solution may ultimately defeat the harmonization purpose of the ePrivacy Regulation.
- The scope of ePrivacy now also includes (i) the processing of electronic communications content for end-users in the EU as well as (ii) the sending of direct marketing communications to end-users in the EU.

EU: A significant reminder on the necessity to process personal data to enter into a contract

- Ever since GDPR came into force on 25 May 2018, businesses have been struggling to efficiently implement its fundamental principles and requirements into their daily business operations. A series of high-profile scandals demonstrated that it is of utmost importance, in particular for Adtech companies and online service providers to clearly assess the most appropriate legal ground to rely upon, in order to legitimize their data processing activities and be transparent about them, in order to avoid potential legal exposure and financial and reputational harms.
- On October 8, 2019, the EU Data Protection Board ("EDPB") issued its final Guidelines to clarify the correct practice of one of the legal grounds justifying the processing of personal data under Art. 6(1)(b) GDPR, notably for the performance of a contract for online services. Accordingly, companies may solely rely upon the performance of a contract as a legal ground to the extent that data processing is strictly necessary for identified legitimate purposes to provide online services to users and/or to enter into a contract, upon payment or free and/or when the processing is necessary to conduct pre-contractual processing activities upon the user's request. In other terms, companies relying on the performance of a contract to justify their processing activities should be able to demonstrate that the processing is in both parties interest and there are no realistic, less intrusive alternatives to achieve the identified and clearly communicated purposes and enter into a contract. Moreover, the processing operations should be limited to what is necessary for the identified and communicated purposes and meet individuals' reasonable expectations. The EDPB notably concludes that the criterion of "necessity" should not be assessed on the sole basis of what is stated in the contract but must satisfy the fairness requirement, under the expectations of the data subjects.
- Further Guidelines are expected on the remaining legal grounds for processing personal data. In the meantime, in case the above-mentioned justification fails, companies should assess whether they can rely on any other legal grounds to legitimize their data processing activities, such as consent, legitimate interest, or an obligation to meet legal requirements and be transparent about them and act accordingly.

EU/US: The Privacy Shield is making progress… but can still be improved

- The Privacy Shield, a self-certification framework, reviewed yearly by the EU Commission and the U.S. Department of Commerce, legitimizes EU-U.S. data transfers despite their different legal systems and data protection regulations. Companies participating in the Privacy Shield framework must comply with data protection principles and ensure that privacy rights of covered individuals can still be exercised once their data is transferred outside of the EU, be it initially to the United States as well as onward transfers.

The Privacist - Volume 2

- On 23 October 2019, the European Commission published its third review report on the functioning of the Privacy Shield, revealing that the U.S. authorities have made substantial improvements over the past year since the last annual review, notably regarding the Privacy Shield implementation and its functioning in order to ensure an adequate level of personal data protection.
- Amongst others, the Commission highlighted that:
  - U.S. authorities are ensuring a significant oversight by performing monthly Privacy Shield compliance verifications on a random sample of the Privacy Shield's participating companies and have proactively increased their enforcement actions in the area of privacy and data protection;
  - Companies have implemented the mandatory mechanisms and successfully handled and responded to the growing number of complaints and requests from EU residents; and
  - A permanent Privacy Shield Ombudsperson has been appointed.
- Nevertheless, the Commission also commented on the room for improvement and, amongst others, recommends for the U.S. authorities to:
  - Further strengthen and shorten the participating organizations' recertification procedure to 30 days instead of approximately three months;
  - Further expand compliance verifications, by better assessing organizations accountability for onward transfers, relying on representative policies and concluded contracts, rather than on questionnaires and responses of contact persons;
  - Provide the Commission and the EU data protection authorities greater transparency regarding ongoing investigations, to better understand and increase convergence of the two systems; and
  - Develop common guidance together with the EU data protection authorities on the definition and treatment of human resources data.

EU/United States: Privacy Shield, vital to trade or a happily never after?

- With around 5,000 participating companies, the Privacy Shield, accompanied by criticism ever since it replaced the Safe Harbor framework, is currently being challenged before the Court of Justice of the European Union ("CJEU"), alongside the Standard Contractual Clauses ("SCCs"), notably in the Schrems II case (Case C-311/18), which again stresses the paramount access powers of U.S. surveillance agencies to Europeans personal data. In addition, three French digital rights groups, La Quadrature du Net (see our other news below), French Data Network, and Fédération FDN are seeking the annulment of the Privacy Shield before the General Court of the European Union for failure to uphold fundamental EU data protection rights given the mass surveillance permitted by U.S. law (Case T-738/16).
- The CJEU judgement in the Schrems II case, expected during the first half of 2020, may invalidate the SCCs and/or the Privacy Shield partially or entirely, rendering both EU-U.S. data transfers completed prior to the judgment, as well as future transfers, illegal. Depending on the outcome, the French digital rights groups' case will then be considered by the General Court, which could invalidate the Privacy Shield as a last resort.
- Provided the uncertainty regarding the outcome of both judgments, amplified by Brexit considerations (see *The Privacist*, Volume 1), the future of data transfers to third countries

is at stake. Consequently, organizations are advised to appropriately consider their risks and data flows, affiliated with potential fines and reputation harms, and to adopt viable tailor made transfer solutions to ensure their future prospects as currently no available mechanisms are in place to legitimize large scale, systematic data transfers outside of the EU.

United States: California Governor Signs Limited Amendments to the California Consumer Credit Privacy Act

- On 11 October 2019, the California Governor Gavin Newsom signed five bills to amend the California Consumer Privacy Act (CCPA), AB 25, AB 874, AB 1146, AB 1355, and AB 1564. The governor's office announced his signing of these bills one day after the California attorney general issued proposed regulations under the CCPA.
- The five bills provide some regulatory relief, but certain key amendments expire on 1st January 2021. Unless the California legislature ultimately decides to extend or modify these amendments, in 2020 or beyond, businesses will need to prepare for the strictest privacy rule in the United States. The amendments providing regulatory relief include the following:
  - **Employee Information Exemption**. The amendments provide an exemption from the CCPA for personal information that is collected in the course of business about a job applicant to the business, or about an employee, owner, director, officer, medical staff member, or contractor of that business, so long as the information is collected and used by the business solely within the context of such relationship. This amendment also exempts personal information that is emergency contact information of these individuals or that is necessary for the business to retain to administer benefits for such individuals, again to the extent that the personal information is collected and used solely in these respective contexts. These exemptions do not apply to the obligation of a business that collects personal information to inform the consumer, at or before the point of collection, as to the categories of personal information collected and the purposes for which such information will be used. They also do not override a consumer's right to recover damages for information security breaches.
    These exemptions expire on 1st January 2021.
  - **Business-to-Business Exemption**. The amendments add an exemption from many of the CCPA's provisions for personal information reflecting a communication or transaction between a business and a consumer where the consumer is a natural person acting as an employee, owner, director, officer, or contractor of a business (including nonprofits) or government agency and whose communications or transactions with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from, such business or government agency. The exemption does not apply to the rule prohibiting discrimination based on the exercise by consumers of their rights and does not override the CCPA's civil money penalty provisions or the rights of consumers to recover damages for information security breaches. This exemption also does not apply to the rule allowing consumers to opt-out from the sale of their personal information or to the opt-in requirement applicable to sales of information regarding consumers who are less than 16 years of age. It appears, however, that businesses would not be required to disclose those opt-out or opt-in rights to consumers given that the section of the CCPA requiring such notices (1798.135) is specifically exempted.
    These exemptions expire on 1st January 2021.

- **Deletion Exception for Certain Warranty or Product Recall Purposes**. The amendments add an exception to the requirement to delete consumers' personal information upon a consumer's request when retention of the information is necessary for the business to fulfill the terms of a written warranty or product recall conducted in accordance with federal law.
- **Expanded Fair Credit Reporting Act Exemption**. The exemption from the CCPA for the sale of certain personal information that is reported in or used to generate a consumer report under the federal Fair Credit Reporting Act ("FCRA") is expanded by the amendments. The CCPA now will not apply to "an activity involving the collection, maintenance, disclosure, sale, communication or use of any personal information" bearing on a consumer's credit worthiness or other characteristics covered by the FCRA definition of consumer report. This exemption covers the foregoing activities by consumer reporting agencies, furnishers of information for use in a consumer report, and users of such consumer reports. This exemption does not apply to the rights of consumers to recover damages for information security breaches.
- **Exclusive Online Businesses**. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information will only be required to provide an email address for consumers to submit requests for information regarding personal information that is collected or sold.
- **Motor Vehicle Dealer and Manufacturer Exception**. A limited exception from consumers' rights to opt-out of the sale of personal information is added by the amendments with respect to vehicle information or ownership information. The consumers' opt-out rights (or opt-in rights in the case of consumers who are younger than 16 years of age) do not apply to vehicle information or ownership information that is shared between a new motor vehicle dealer and the vehicle's manufacturer if the information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall conducted pursuant to federal law. However, the new motor vehicle dealer or vehicle manufacturer may not sell, share, or use such information for any other purpose.

- The enacted bills also correct a number of drafting errors and clarify certain issues. With respect to clarifications:
  - As part of determining that a consumer's request for information is a "verifiable consumer request," a business may require authentication of the consumer that is "reasonable in light of the nature of the personal information requested."
  - The definition of "*personal information*" is amended to clarify that it includes specified information when it is "*reasonably capable of being associated with*" a particular consumer or household, as opposed to simply "*capable of being associated with*" a particular consumer or household.
  - The definition of "*personal information*" also is amended to clarify that it does not include consumer information that is de-identified or aggregate consumer information.
  - Whether one characterizes it as a clarification or a new exception, the CCPA, as amended, specifically provides that it shall not be construed to require a business to collect personal information that it would not otherwise collect in the ordinary course of business or to retain personal information for longer than it would otherwise retain such information in the ordinary course of business.

- The amendments direct the California attorney general to establish rules and procedures on how to process and comply with verifiable consumer requests for specific pieces of personal information relating to a household in order to address obstacles of implementation and privacy concerns. Given that the governor signed these amendments one day after the attorney general proposed regulations, it seems reasonable to assume that additional regulations will be proposed.
- The CCPA takes effect in just a few months, on 1st January 2020. While the California attorney general may not bring an enforcement action under the CCPA until six months after the publication of final regulations on 1st July 1 2020, whichever is sooner, businesses that will be subject to the CCPA need to prepare for the 1st January 2020 effective date.
- As a first step, a business should identify all of the covered "*personal information*" that it "*collects*," "*sells*," or discloses for business purposes. Businesses also will need to coordinate with their vendors and other third parties with which they share consumers' personal information, or from which they obtain personal information, and in many cases adjustments to existing contracts with these third parties might be needed. In addition, covered businesses will need to develop systems to store the covered information in ways that allow the business to address consumers' rights, implement systems to respond to consumers' requests for information or deletion of their personal information, develop the required disclosures, and begin training of relevant staff. Finally, every business will need to make certain decisions, including whether to treat all information about individuals the same way for storage and similar purposes whether or not relating to a covered "*consumer*" (which depends on the individual's residency) and whether to extend CCPA rights to all individuals regardless of their California residency.

Italy: The new Code of conduct for credit reporting systems issued by the Italian Supervisory Authority

- The Italian Supervisory Authority (*Garante per la protezione dei dati personali*, "Garante Privacy") has introduced new rules on consumer credit, loans, and new types of financing, providing greater safeguards for consumers registered in credit databases as well as transparency on the functioning of algorithms that analyze financial risk in light of emerging technologies including FinTech services.
- On 12 September 2019, upon proposal of a group of trade associations, the Garante Privacy adopted the new "Code of conduct for credit reporting systems operated by private entities regarding consumer credit, creditworthiness and punctuality in payments" (the "Consumer Credit Code" available in Italian here) for the Credit Reporting Systems ("CRS"). Replacing its pre-GDPR 2004 version, this Code is the second code of conduct introduced by the Garante Privacy following the adoption, last June, of the "Code of conduct for the processing of personal data relating to commercial information" (the "Commercial Information Code" available in Italian here). The Commercial Information Code, initially submitted by the National Association of Commercial Information and Credit Management Companies ("ANCIC"), was the first code of conduct ever adopted in Europe since GDPR's entry into force pursuant to Art. 40 GDPR.
- The Commercial Information Code regulates the processing of personal data of individuals for commercial purposes coming directly from the data subjects as well as from public registers, lists, deeds, or documents known by anyone or publicly accessible (e.g., the Internet and newspapers). In order to process such data, service providers

are required to inform the data subjects about the data processing activities by submitting a privacy information notice to be published on the ANCIC website. Instead, when the processing of personal data aims at obtaining information on the commercial reliability of checked persons, the consent of data subjects is not required as providers act on the legal basis of their legitimate interest since they provide commercial information services. The Commercial Information Code also sets up a new independent monitoring body ("OdM"), external to the ANCIC, to verify the compliance by the adherent providers to the provisions of the Commercial Information Code. Such body has also been introduced by the Consumer Credit Code.

- The Consumer Credit Code sets out a new regulatory framework that aims at adapting the credit risk analysis to the challenges brought by the digital economy within the new European privacy regulatory framework. Indeed, these new rules address not only personal data pertaining to loans and mortgages but also different forms of leasing, long-term rentals, and innovative private sector loans, managed via through FinTech platforms. Such data are contained in CRS, which acts as databases recording data relating to requests for financing, especially those concerning payments, delays, or default of instalments. These databases are managed by entities which make the relevant personal data available to other entities (e.g., credit institutions, financial institutions, sellers selling goods on instalment basis, telecommunication service providers, etc.) and which may assess the circumstances for the provision of a loan and/or other forms of financing based on such data. The scope of the Consumer Credit Code is to ensure that the above assessment activity is carried out by guaranteeing all the necessary protection for the consumers personal data recorded in the CRS.
- The Consumer Credit Code sets forth that only the data which would be strictly necessary to the credit risk assessment purposes may be processed, without necessitating any specific consent by the data subjects, through the provision of complete and timely information to the data subjects. Specifically, within the context of each request reported to the CRS, the following data may be processed:
  - identification, personal and sociodemographic data (for example: tax code, VAT number, contact details, identity documents, health card, Iban code, data relating to employment/profession, income, sex, age, residence/domicile, marital status, family unit);
  - data related to the request/report, descriptive, in particular, of the type of contract, the amount due, the methods of payment and the status of the request or execution of the contract;
  - accounting data, relating in particular to uses or payments, their periodic performance, debt exposure (including residual debt), and a summary of the accounting statement of the report; and
  - data relating to litigation and debt recovery activities, the assignment of the receivable or exceptional events that affect the subjective or financial situation of the parties concerned.
- Both Codes, which refer exclusively to the processing of personal data of natural persons limited to the Italian territory, prohibits the processing of special categories of personal data as well as data relating to criminal convictions and offences or related security measures, with an exception for the Commercial Information Code relating to the criminal data that originate from public registers.
- The purposes of the processing pursuant to the Consumer Credit Code include the verification, including comparative verification, of the predictivity of the information

contained in the CRS, the development and verification of models, statistical analysis factors, algorithms, indicators, and scores as well as aggregate, anonymous, or pseudonymous processing in order to satisfy the statistical, regulatory or product or service development needs of the CRS participants. The Consumer Credit Code requires that any such use of personal data be subject to appropriate security measures and techniques in order to ensure the reliability of the systems as well as the safe management of the data (for example, through appropriate encryption or pseudonymisation techniques). The same principle regarding the adoption of security measure also applies to the Commercial Information Code based on the fact that participating providers will have to operate according to a risk-based approach by adopting technical, procedural, physical, and organizational measures to prevent or minimize the risks of destruction, loss, modification, and unauthorized disclosure or access to personal data.

- In the approval decision of the Consumer Credit Code, the *Garante Privacy* required the operators within CRS to make some changes to the functioning of the monitoring body established by the Consumer Credit Code in order to strengthen its independence and autonomy from sector-related companies.
- Finally, the subscribers to the new Consumer Credit Code have committed themselves to comply forthwith with the rules and principles therein contained within six months from the approval of the Code. Nevertheless, both codes will become fully effective only upon completion of the accreditation procedure of the OdM following a favorable opinion of the EU Data Protection Board ("EDPB").

Germany: DSK issues guidelines for setting fines under Art. 83 GDPR

- The Conference of Germany's Independent Data Protection Authorities (Datenschutzkonferenz, "DSK") has published a concept for the computation of fines pursuant to Art. 83 GDPR in order to allow transparent, fair and comprehensible fines for GDPR violations (available in German here). The concept does only apply to administrative fines against companies in Germany and is only an interim solution until the EDPB decides on an EU-wide solution.
- The concept establishes a five-step assessment for calculating administrative fines:
  - First, the whole company group is matched to one of four pre-defined entity sizes ((i) mini companies (annual turnover under EUR 2m), (ii) small companies (annual turnover under EUR 10m), (iii) medium sized companies (annual turnover under EUR 50m) and (iv) large companies (annual turnover above EUR 50m));
  - In a second step, the aggregated annual turnover of the relevant business unit within the company group is assessed in relation to the entity size assessed in Step 1;
  - In the third step the calculation result of Step 2 is divided by 360, i.e. an average daily value;
  - The fourth step applies a factor to the result of Step 3, depending on the severity of the breach (ranging from factor 1-2 for low level breaches of Art. 83 para 4 GDPR up to factor 12 for very severe breaches of Art. 83 para 5 and 6 GDPR); and
  - Step 5 ultimately allows to take into account individual circumstances not yet covered by Step 4 (in particular those laid down in Art. 83 para. 2 GDPR).
- As this is the first attempt of national supervisory authorities to provide comprehensible guidelines for the calculation of administrative fines, it remains to be seen whether courts will abide by this concept in case of a judicial challenge of the amount of an

issued fine and whether other EU countries and, in particular, the EDPB will follow such approach in the future.

France: Supervisory Authority's White List of Processing Exempt from Data Protection Impact Assessment

- On 22 October 2019, the French Supervisory Authority (Commission Nationale de l'Informatique et des Libertés or "CNIL") published its deliberation regarding processing operations exempt from the requirement of a Data Protection Impact Assessment ("DPIA") under Art. 35(5) GDPR. The deliberation was modified accordingly to previous EDPB's opinion on 10 July 2019.
- Are exempt the following processing operations:
  - carried out solely for human resources purposes and in accordance with applicable law, only for staff management of organizations employing less than 250 persons, with the exception of the use of profiling;
  - regarding supplier relationship management;
  - carried out in accordance with applicable law relating to the municipalities' electoral register management;
  - intended for the management of activities of employee representative committee;
  - carried out by an association, foundation, or any other nonprofit institution for its members and donors management in the context of its usual activities, excluding special categories of personal data under Art. 9 GDPR;
  - health data necessary for patients management by a health professional working individually in a medical practice, pharmacy or medical biology laboratory;
  - carried out by lawyers in the individual exercise of their profession;
  - carried out by commercial courts' clerks over the course of their professional activities;
  - carried out by notaries to carry out their professional activity and drafting notarial office documents;
  - management of school, extracurricular and childcare services by local authorities and legal persons;
  - solely for the purpose of physical access controls and working time schedules for the computation of working time (excluding the use of biometric device and the processing of data revealing sensitive or highly personal data); and
  - relating to breathalyzer tests strictly regulated by applicable law and implemented in the context of transport activities and for the sole purpose of preventing the operation of a vehicle under the influence of alcohol or narcotics.

France: Online Targeted Advertising: Administrative Supreme Court validates the French Supervisory Authority's action plan

- With the ePrivacy Regulation still under discussion (with its latest draft dated 4 October 2019, available here), cookies keep raising questions and adding fuel to the fire of debates.

The Privacist - Volume 2

- GDPR as well as the French Data Protection Law, reinforced consent requirements: while simple scroll through used to be deemed sufficient to express consent in the context of placing cookies and other tracking devices on a user's terminal, GDPR now requires that consent must be active. This revolution in the business of online advertising means that market players must now ensure that users explicitly consent to the use of cookies or other tracking devices prior their placement for behavioral advertising purposes.
- In July 2019, the French Supervisory Authority (Commission Nationale de l'Informatique et des Libertés or "CNIL") adopted a deliberation (available in French here) clarifying the legal framework applicable to cookies and related technologies including new consent rules for targeted advertising. In addition, the CNIL initiated consultations with professionals from the online advertising industry, in order to define best practices to obtain consent by the first quarter of 2020. Once these new best practices are determined, industry players would have six months to comply and implement these practices.
- La Quadrature du Net and Caliopen (French data protection and consumer associations) challenged this transition period before the French administrative Supreme Court ("Conseil d'Etat").
- The associations argued that this delay characterized the CNIL waiving its duty to sanction. They also took issue with the CNIL's continued tolerance, until new rules are established of continued browsing being validly construed as "consent." They alleged that this tolerance was contrary to GDPR, especially to the requirement of a clear affirmative action for consent. Finally, the associations claimed that the action plan was contrary to the right to privacy and data protection as set out under the European Convention on Human rights and the European Union Charter of fundamental rights.
- The Conseil d'Etat upheld the CNIL's action plan in October 2019, considering that the CNIL had a broad discretionary power to sanction or not. They noted that this delay was merely a practical adaptation of the legislation, in order to enable market players to achieve the required technical modifications. In addition, during this transition period, the CNIL would continue to monitor overall compliance with GDPR. Therefore, the measures taken by the CNIL could not be construed as a *"disproportionate interference in fundamental rights."* The French jurisdiction deemed the delay reasonable and considered that the immediate exercise of a power to sanction would not result in any faster compliance by market players.

The Privacist - Volume 2

EU: GDPR Fine Tracker (October)

Country	Authority	Date	Fine (EUR)	Fine (original currency)	Controller/Processor	Sector	Quoted Article	Ground	Summary	Additional information
SPAIN	Spanish Data Protection Authority (aepd)	1 October 2019	18 000,00 €		Vueling Airlines	Services	Art. 5, 6 GDPR	Insufficient legal basis	The company's website did not allow users to continue navigation without consenting to the cookies. The data subjects had no possibility to refuse the use of tracking files on their devices.	link
GREECE	Hellenic Data Protection Authority (HDPA)	7 October 2019	200 000,00 €		Telecommunication service provider	IT/Tech	Art. 5(1)c), 21(3), 25 GDPR	Noncompliance with processing principles	Despite the refusal to receive telemarketing calls, a large amount of customers were subject to unsolicited calls. Moreover, due to some technical difficulties, over 8 000 of the accounts were not deleted upon	link

The Privacist - Volume 2

									the users' requests.	
ROMANIA	Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	9 October 2019	20 000,00 €		Credit company	Financial	Art. 32, 33 GDPR	Insufficient security measures	(joint decision) Raiffeisen Bank effectuated their credit scoring on the basis of the personal data provided to the bank by the Vreau Credit platform's employees via WhatsApp. Subsequently, the bank was sending the results to the platform via WhatsApp as well.	link
ROMANIA	Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	9 October 2019	150 000,00 €		Raiffeisen Bank SA	Financial	Art. 32 GDPR	Insufficient security measures	(joint decision) Raiffeisen Bank effectuated their credit scoring on the basis of the personal data provided to the bank by the Vreau Credit platform's employees via WhatsApp. Subsequently, the bank was	link

The Privacist - Volume 2

									sending the results to the platform via WhatsApp as well.	
SPAIN	Spanish Data Protection Authority (aepd)	16 October 2019	8 000,00 €		Iberdola Clientes	Other	Art. 31 GDPR	Lack of cooperation with Data Protection Authority	The company in the energy sector did not respond to the DPA's request about the possibility to add data of a person requesting to change a supplier to the solvency list.	link
SPAIN	Spanish Data Protection Authority (aepd)	16 October 2019	60 000,00 €		Xfera Moviles	IT/Tech	Art. 5, 6 GDPR	Insufficient legal basis	The company has used personal data without a valid legal basis to conclude a telecom contract and continued data processing even after a person requested to restrict such processing.	link
ROMANIA	Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	17 October 2019	2 500,00 €		Industry	Services	Art. 5(1)c), 6, 12, 13 GDPR	Unsatisfactory information obligations	The controller was unable to prove that data subjects were correctly informed about the CCTV recording.	link

The Privacist - Volume 2

AUSTRIA	Austrian Data Protection Authority (dsb)	29 October 2019	18 000 000,00 €		Austrian Post	Other	Art. 5 (1) a, 6 GDPR	Insufficient legal basis	Austrian Post has illegally used marketing data to create the users' profiles on the platform and to estimate their political affiliation. Their findings were sold to other companies.	link

K&L GATES

The Privacist - Volume 2

Authors:

Natali Adison
natali.adison@klgates.com
+32.2.336.1934

Claude-Étienne Armingaud
claude.armingaud@klgates.com
+33.1.58.44.15.16

Eleonora Curreri
eleonora.curreri@klgates.com
+39.02.3030.2980

Alessandra Feller
alessandra.feller@klgates.com
+39.02.3030.2939

Jeremy McLaughlin
jeremy.mclaughlin@klgates.com
+1.415.882.8230

Thomas Nietsch
thomas.nietsch@klgates.com
+49.(0)30.220.029.408

Linda Odom
linda.odom@klgates.com
+1.202.778.9363

John ReVeal
john.reveal@klgates.com
+1.202.778.9055

Judith Rinearson
judith.rinearson@klgates.com
+1.212.536.3928

Lucile Rolinet
lucile.rolinet@klgates.com
+33.01.58.44.15.43

K&L GATES

K&L Gates is a fully integrated global law firm with lawyers located across five continents. The firm represents leading multinational corporations, growth and middle-market companies, capital markets participants and entrepreneurs in every major industry group as well as public sector entities, educational institutions, philanthropic organizations and individuals. For more information about K&L Gates or its locations, practices and registrations, visit www.klgates.com.