July 2019 EU affairs newsletter

French Data Protection Authority CNIL releases online marketing action plan

France's data protection authority, the CNIL, has released its action plan for online marketing for 2019–20. The CNIL said its focus on online marketing is in response to complaints made by individuals and organizations and as marketing professionals seek to learn about their obligations under the EU General Data Protection Regulation. The agency announced it will publish new guidelines in July and will consult with stakeholders in order to develop new recommendations on the operational aspects of consent collection, which the CNIL hopes to publish by December or early next year.

Link to CNIL press release : https://www.cnil.fr/en/online-targeted-advertisement-what-action-plan-cnil

Italian DPA fines Facebook for data protection breach in Cambridge Analytica issue

Italy's data protection authority, Garante, announced it had fined Facebook 1 million euros over Cambridge Analytica, Politico reports. The agency found 57 citizens downloaded the This Is Your Digital Life app tied to Cambridge Analytica; however, the DPA found no information had been passed onto the firm. The fine is the largest Facebook had to face for Cambridge Analytica, as it surpasses the 500,000 GBP penalty issued by the U.K. Information Commissioner's Office. The fine issued by Garante was not issued under the EU General Data Protection Regulation.

CJUE hearing on "Schrems II" and Standard Contractual Clauses

Ireland's data protection authority came under fire during a hearing at the Court of Justice of the European Union on July 9th over its refusal to take a decision on whether Facebook could transfer the personal data of Europeans to the United States.

EU institutions, national governments and industry groups joined Austrian privacy activist Max Schrems and even the Irish government in lining up to criticize the Dublin-based regulator, which had deferred the matter to Ireland's highest court.

"The Data Protection Commissioner has the necessary power to suspend or prohibit data flows," a representative for the Irish government said, referring to Facebook's data transfers to the U.S., which were the subject of a complaint brought by Schrems in 2013. "We acknowledge the difficulty of the task, but it should not mean all standard contractual clauses should be deemed invalid."

Instead of deciding on the case, the Irish Data Protection Commission (DPC) asked its country's national courts to determine whether so-called standard contractual clauses — complex legal mechanisms that allow thousands of companies to move data from Europe to the U.S., Asia and elsewhere — were valid.

The Irish High Court then referred the case to the Court of Justice of the European Union (CJEU), which now has to assess whether they violate Europeans' fundamental right to privacy, leading to Tuesday's hearing. In his original complaint, Schrems sought to get Facebook to stop sending Europeans' personal data to the United States on the basis that it would be subject to surveillance from intelligence bodies such as the National Security Agency.

The Privacy Shield is a transatlantic data flow agreement allowing companies to transfer European personal data from the EU to the U.S. It replaces the Safe Harbor, which was struck down by the CJEU in late 2015.

Data shutdown fears

Schrems' complaint focuses squarely on Facebook and the so-called standard contractual clauses it used to transfer personal data to the United States.

But the judges in Luxembourg, whose final decision is expected in early 2020, could make a ruling on the validity of standard contractual clauses in general. Companies worry that a ruling to invalidate the clauses could turn off data transfers from Europe to the U.S. overnight and affect flows to other parts of the world such as Asia and South America.

"The effect [of an invalidation of standard contractual clauses] on trade would be immense and would have World Trade Organization implications for the EU," Facebook's lawyer told the court. "There is no evidence that Facebook's transfers are under any particular risks."

Both the tech giant and the U.S. government made the argument that ruling on a foreign surveillance regime is not within the court's scope. Europe's sweeping privacy reform — the GDPR — does not give the EU the mandate to "conduct a worldwide enquiry" of surveillance regimes across the world, a representative for the U.S. government said.

Meanwhile, the Irish regulator argued that the European court should invalidate standard contractual clauses because they do not offer sufficient remedies for users whose data has been collected by U.S. intelligence agencies.

Ganging up against the DPC

Schrems had originally complained to Ireland's DPC, which is in charge of Facebook, given the location of the company's European headquarters in Dublin.The regulator questioned the validity of standard contractual clauses in general, and the High Court asked the CJEU to rule on the compliance of such mechanisms in general with the Charter of Fundamental Rights.

But the Austrian activist did not want to question the validity of all standard contractual clauses."We agree with the DPC [on U.S. surveillance], but not on the radical solution. The solution is not for the court to invalidate standard contractual clauses but for the Data Protection Commissioner to enforce them," his lawyer said.

The European Commission, EU governments and tech lobby BSA-The Software Alliance, which represents companies such as Apple, IBM and Microsoft (but not Facebook), defended the overall validity of the transfer mechanism. "This case is not about U.S. laws but about who's responsible for what. What's the responsibility of the European Commission, the DPC, national courts ..." the Commission said. The Netherlands and the U.K. echoed Ireland's comments about the DPC's role in stopping data transfers.

Privacy Shield's shadow

For the hearing, the court also asked a series of questions about the legality of the separate Privacy Shield transatlantic data flow agreement. Judges insisted the two cases are linked.

A separate hearing on the Privacy Shield agreement at the EU's General Court has been postponed pending a judgment in the case heard on July 9th .

The EDPB also expressed some known concerns about effective remedies for European citizens in the U.S. The board "cannot state that the Ombudsperson constitutes an effective remedy," Jelinek told the court, referring to the person in charge of handling complaints by European citizens.

Unsurprisingly, the Commission defended its decision to strike an agreement with Washington on data flows. But it struggled to answer to the judge's questions about whether U.S. intelligence agencies have access to content data from EU users.

National governments, including Ireland, urged judges to "confine their examination" to standard contractual clauses.

The conclusions from the court's advocate general are expected December 12.

French DPA updates guidelines on cookies post GDPR

The French DPA CNIL has tightened its guidelines on cookies to comply with GDPR and EDPB guidelines on consent. Therefore, continuation of browsing will not be deemed as valid consent anymore and that cookies walls are not valid either. These new guidelines replace the version that had been adopted in 2013, and digital and advertising companies have one year to become compliant.

Link to the text published (in French):

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038783337&dateTexte=&categorieLien=id

CJEU: Websites jointly liable for data use via Facebook 'Like' button

The Court of Justice of the European Union ruled third-party websites are jointly responsible for the processing of personal data under EU privacy rules when users click on a Facebook “Like” button embedded on a third-party site, Bloomberg reports. The court responded to a case in which an online fashion retailer was accused of violating EU law through its use of the Like plugin. The case was launched before the EU General Data Protection Regulation went into effect. The court ruled a website can be held jointly responsible for “the collection and transmission to Facebook of the personal data of visitors to its website.” Facebook Associate General Counsel Jack Gilbert said in a statement the company is reviewing the decision and will work with its partners to ensure continued compliance with the law.

E-privacy

New Council paper from Finnish Presidency to be discussed in working group in September

The Finnish Presidency unveiled on July 26th a new working document for the Council telecommunication working group to discuss early September on the draft e-privacy regulation. This working paper concentrates on article 5 to 10 and clearly specifies that articles 12 to 16 won’t be discussed at the next TELE WG in September.

It also takes into account the position unveiled by the German delegation which didn't agree on the former proposal done by the Romanians on article 6. The Finnish Paper therefore proposes that article 6 has been divided in 4 articles:

- **article 6** dealing with processing of all electronic communications data (ex. 6(1)),
- **article 6a** dealing with processing of electronic communications content (ex. 6(3)),
- **article 6b** dealing with processing of electronic communications metadata (ex. 6(2)),
- **article 6c** dealing with further processing of electronic communications metadata (ex.6(2a).

Throughout article 6, the Presidency has deleted references to the processing only 'for the duration necessary for a specific purpose' and only 'if the purpose cannot be fulfilled by processing of information made anonymous'. New **art. 6(2)** now clarifies that these principles are universally applicable to all types of processing under articles 6 to 6c. The Presidency's reading is that this would anyway be the case by virtue of the principles established by the GDPR. Also the concept of anonymisation in relation to legal entities has been clarified in **rec. 15a.**

The link to the overall text can be seen here

Below is a snapshot of changes proposed to article 16 on direct marketing communications

Article 16 on direct marketing has been amended as follows by the Finnish paper

Article 16

Unsolicited and ~~D~~direct marketing communications

1. Natural or legal persons ~~may~~ **shall be prohibited from** us**eing** electronic communications services for the purposes of sending ~~**or presenting**~~ direct marketing communications to end-users who are natural persons ~~that~~ **unless they** have given their consent.

2. **Notwithstanding paragraph 1, ~~W~~w**here a natural or legal person obtains ~~**electronic**~~ contact details for electronic ~~**mail**~~ **message** from ~~**its customer**~~ **end-users who are natural persons**, in the context of the ~~**sale**~~ **purchase** of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these ~~**electronic**~~ contact details for direct marketing of its own similar products or services only if ~~**customers**~~ **such end-users** are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection **of such end-users' contact details** and**, if that end-user has not initially refused that use,** each time ~~**that**~~ **when a natural or legal person~~s~~ sends a message to that end-user for the purpose of ~~such~~ direct marketing ~~communication is sent or presented~~**.

2a. **Member States may provide by law a set period of time, after the sale of the product or service occurred, ~~that~~ within which a natural or legal person may use ~~its customer's~~ contact details of the end-user who is a natural person for direct marketing purposes, as provided for in paragraph ~~2 only where the sale of the product or service occurred not more than twelve months prior to the sending of an electronic message for direct marketing~~.**

3. Without prejudice to paragraphs 1 and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall~~:~~

~~(a)~~ present the ~~identity of a~~ **calling** line **identification** on which they can be contacted~~; or~~**.**

~~(b)~~**3a.** **Member States may require natural or legal person using electronic communications services for the purposes of placing direct marketing calls to** present a specific code ~~/~~or prefix identifying the fact that the call is a **direct** marketing call **in addition to the obligation set out in paragraph 3. Member State requiring the use of such a specific code or prefix shall make it available for the natural or legal persons who use electronic communications services for the purposes of direct marketing calls**.

4. Notwithstanding paragraph 1, Member States may provide by law that the placing of direct marketing voice-to-voice calls to end-users who are natural persons shall only be allowed in respect of end-users who are natural persons who have not expressed their objection to receiving those communications.

5. Member States shall ensure, in the framework of Union law and applicable national law, that the legitimate interest of end-users that are legal persons with regard to ~~unsolicited~~ **direct marketing** communications sent ~~or presented~~ by means set forth under paragraph 1 are sufficiently protected.

6. Any natural or legal person using electronic communications services to ~~transmit~~ send ~~or present~~ direct marketing communications shall**, each time a direct marketing communication is sent ~~or presented~~:**

(a) **reveal his or its identity and use ~~true~~ effective return addresses or numbers;**

(b) inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the **direct marketing** communication is ~~transmitted~~ sent ~~**or presented;**~~

(c) ~~**and shall** provide the necessary information for recipients **end-users who are natural persons** to exercise their right to **object or to** withdraw their consent, in an easy manner **and free of charge**, to receiving further **direct** marketing communications;~~

(d) **clearly and distinctly give the end-users who are natural persons a means to object or to withdraw their consent, free of charge, at any time, and in an easy and effective manner ~~and free of charge~~, to receiving further direct marketing communications, and shall provide the necessary information to this end. This means shall also be given at the time of collection of the contact details according to paragraph 2. It shall be as easy to withdraw as to give consent.**

~~**6a. Advertisements on a website that are displayed to the general public and do not require any contact details of end-users should not be subject to this article.**~~

~~7. The Commission shall be empowered to adopt implementing measures in accordance with Article 26(2) specifying the code/or prefix to identify marketing calls, pursuant to point (b) of paragraph 3.~~

About FEBIS– Federation of Business Information Services

Benefiting from the opening of markets within Europe and overseas, world-wide business has experienced substantial growth. As business grows so does the demand for business information intelligence for cross-border business activities.

In 1973, leading European credit information agencies joined forces to form the Federation of Business Information Services FEBIS (initially known as FECRO), with its registered office in Frankfurt. Today, FEBIS has developed into a sizable organization comprising more than 100 members from all over the world involved in providing Business Information and credit information services of national and International importance.

As the industry association, FEBIS strives to look after common interests of its members. While monitoring new legislation like data protection laws and insolvency laws, FEBIS also oversees and the application of public sources and information.