April 2019 EU affairs newsletter

French DPA CNIL survey on PIA software

One year into the existence of the PIA software, CNIL made available a survey in order to understand precisely how the tool is used, assess user satisfaction, and pinpoint possible improvements. This information will be used to guide future software developments. The survey was open until 22 April included. If you wish to download the last version of the software, the link is available on the PIA tool page.

Polish DPA fine on failure to comply with information notification obligation under art of the GDPR

On March 26th the Polish Data Protection Authority (UODO) issued a 220 k€ fine against a digital marketing company (Bisnode Poland) for failure to comply with information notification obligation under art 14 of the GDPR. Thought the case is challenged by the company and it might take time to be judged in appeal, the impact of the decision could resonate very strongly in the business information and digital marketing community because aside from the fine itself , the costs associated with compliance requirements if the DPA interpretation is upheld by other DPAs could amount to millions of euros.

Below is a very rough summary of the decision, you can have more extensive information from the EDPB press release and also from the following press article: https://techcrunch.com/2019/03/30/covert-data-scraping-on-watch-as-eu-dpa-lays-down-radical-gdpr-red-line/

- The Polish DPA is saying that the company failed to comply with the information notification obligation of art 14 of the GDPR because it did not actively contact the almost 6 million people they have in their databases to warn them that their personal data was being processed. This inter alia concerns sole entrepreneurs but also directors or company managers whose personal data is encompassed into business registers which are used as a data source by the company.
- The company had issued a notice on its website warning about data subjects rights and the possibility to exert them, but did not contact individually all persons– they sent out emails

when they had email addresses but did not reach out to all other contacts because it would have been a disproportionate effort . The UODO is saying that for contacts where there was a postal mail or a telephone number, the company should have contacted them individually and is challenging the fact that this is representing a disproportionate effort.

- The whole question of what constitutes a disproportionate effort will surely be at the centre of the judgement and the question of active manner of notification vs disproportionate effort is key : there are some caveats included in article14 allowing for a data controller to dispense with the requirement to inform data subjects if doing so "proves impossible or would involve a disproportionate effort " but the DPA is saying this would not apply to commercial entities like B2B marketing business..
- The decision is putting a big threat on the way business information providers re-use information coming from public sources and represent a big challenge towards the treatment of sole entrepreneurs' data in business and credit reference information environment. The fact that the Polish DPA requires art 14 information notifications to be communicated individually to all natural persons (including sole traders and business managers) would definitely be a big burden for all actors and could set resonance.

At the last FEBIS regulatory committee conference call, members who were present agreed that the issue was important and that therefore it would be good to investigate how the company was using the data (for what use case) and how FEBIS members are fulfilling the information obligation under art 14 of the GDPR.

FEBIS therefore asked its members to provide information on the 2 following questions :

1. **Whether they actively & personally notify data subjects with their privacy notices and if so when**
2. **Whether they have any formal or informal statements from their data protection authorities on the issue or the scope of exceptions to Art. 14**

Discussion on this issue will take place during the Regulatory Session of the FEBIS Spring Meeting in Riga.

Czech Republic draft laws implementing GDPR agreed in Parliament

The Czech Chamber of Deputies approved two bills adapting Czech law to the EU General Data Protection Regulation — the Data Protection Act and the Accompanying Act. This comes more than nine months after the GDPR came into effect. The bills will now be presented to President for his signature. The Data Protection Act fully replaces the current Czech Data Protection Act and includes several local derogations and exceptions (primarily for the public authorities). The act also includes provisions on the constitution and powers of the Czech Data Protection Office. In addition, it transposes Directive 2016/680, which regulates the processing of personal data related to preventing and investigating crimes and regulates the processing of data while ensuring the defense and security mechanisms of the Czech Republic. The Accompanying Act affects and amends more than 30 laws in connection with the GDPR and Directive 2016/680.

There were extensive discussions about the acts in the Chamber of Deputies, and the deputies discussed more than 30 amending proposals.

The approved bills bring about a few important changes (besides legislative-technical changes), mainly:

- Broad exceptions for the processing of personal data for compatible purposes in case of public interest and where the controller is subject to the legal obligation.
- Broad possibilities for restricting data subjects' rights in matters of public interest and regarding the enforcement of private claims.
- ***The possibility of the processing of the national identification numbers (birth certificate number) for the enforcement of private claims***.
- ***The possibility of informing data subjects online (via the publication of information on the internet), if the processing of data is based on law and in the public interest.***
- The exceptions for processing personal data for scientific or historical research or statistical purposes.
- The possibility for controllers to inform data subjects of corrections, limitations and liquidation of data just by an update of initial records in some instances.
- A definition of public subjects who are obliged to name a data protection officer.

Most importantly, the deputies have completely abolished fines for all public authorities and bodies. The scope of this wide exception remains to be interpreted, but it will most likely cover all governmental bodies, ministries, municipalities, schools, public hospitals, and other controllers and processors established by a legal act for the fulfillment of duties in public interest. In addition, the Czech Data Protection Office is, as a general rule, allowed to drop minor offenses without initiating formal proceedings and without notifying the person concerned.

Apart from other things, the deputies have not approved the widely discussed lowering of the age limit to 13 years for the necessity of the consent of a legal representative for using online services. Finally, the age limit for children's consent is raised to 15 years.

A hardly visible though important change is the extension of the authority of the Czech Data Protection Office. According to the Accompanying Act, the office has gained new powers in the area of free access to information. Among other things, the office obtains a new power to issue (a directly enforceable) instruction to subordinate authorities to provide information (the change affects primarily Act 106/1999 Coll., on free access to information). The office would lead the review procedure of provision of information and has been authorized to issue these kinds of orders. These provisions should come into effect from Jan. 1, 2020.

The act is now waiting for the signature of the president to be fully approved and effective sometime in May 2019.

Data protection

Finnish Data Protection Ombudsman processes two cases on financial credit and GDPR

Two cases concerning Svea Ekonomi, a financial credit company , have been processed at the Office of the Data Protection Ombudsman. As a result, **the Data Protection Ombudsman has ordered the company to correct its practices in the processing of personal data related to the assessment of creditworthiness, the right of inspect one's own personal data and notification practices**.

One of the cases concerning Svea Ekonomi has been processed at the Office of the Data Protection Ombudsman as a complaint made by a single data subject. It concerned the personal data used to assess creditworthiness and the data subject's right to inspect data concerning them. Furthermore, the Office of the Data Protection Ombudsman began to process the matter concerning the company's notification practices upon its own initiative.

In its decision, the Data Protection Ombudsman stated that the use of a categorical upper age limit in assessing creditworthiness is not acceptable under the definition of credit information set out in the Credit Information Act. The mere age of the credit applicant does not describe their solvency, willingness to pay or ability to deal with their commitments. **Based on the account submitted by the company, the credit applicant's financial position has not been taken into consideration at all in the automatic processing of the credit application.**

In the second case, the Data Protection Ombudsman also pointed out that the company's on-line credit decision service **should be considered automatic decision-making** of the kind referred to in Article 22 of the GDPR, in which the decision is essential in order to conclude or implement an agreement between the company and the credit applicant.

In its decision, the Data Protection Ombudsman ordered Svea Ekonomi to change the processing of personal data related to assessing creditworthiness. **The company must also provide the private person having complained about the matter with information on the logic employed in automatic decision-making, its role in making the credit decision as well as its consequences for the credit applicant**.

The Office of the Data Protection Ombudsman has also investigated Svea Ekonomi's notification practices related to the automatic decision-making system used to assess creditworthiness. The Data Protection Ombudsman stated that the current notification practices do not sufficiently specify the logic of data processing so that the credit applicant could understand the grounds for the decision and ordered that such notification practices be changed.

Based on the Data Protection Ombudsman's decision, Svea Ekonomi must notify by 30 April 2019 how it has changed its processing of personal data. According to the Office of the Data Protection Ombudsman, Svea Ekonomi has not applied for change in the decision, so the decision is legally enforceable.

Link to the decision in Finnish : https://tietosuoja.fi/artikkeli/-/asset_publisher/tietosuojavaltuutettu-maarasi-svea-ekonomin-korjaamaan-kaytantojaan-henkilotietojen-kasittelyssa

Data protection

European Data Protection Board public consultation on guidelines on processing of personal data under art 6(1)b in the context of online services provision

The European Data Protection Board has issued a public consultation on its draft **Guidelines 2/2019** on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects.

Comments should be sent to EDPB@edpb.europa.eu by **24/05/2019** at the latest.

Link to the consultation : https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-22019-processing-personal-data-under-article-61b_en

The European Commission has also commissioned a study on certification mechanisms unveiled in articles 42 and 43 of the GDPR (study available here).

Finance

US draft Algorithmic Accountability Act

Pressure continues to mount in the U.S. to keep data privacy and protection at the forefront. With the California Consumer Privacy Act set to go into effect in January 2020, consumers, businesses, governmental entities and other third parties are closely watching the data privacy developments taking shape in the U.S.

On April 10th 2019 , two US Senators proposed the Algorithmic Accountability Act of 2019 in the U.S. Senate, with a House of Representatives equivalent sponsored by Rep. Yvette Clarke, D-N.Y. The bill, which is also referred to as S.1108, is influenced by the GDPR and CCPA, and directs the Federal Trade Commission to require entities that use, store or share personal information to conduct automated decision system impact assessments and data protection impact assessments.

Those entities that would be mandated to adhere to the Accountability Act shall be referred to as "covered entities." The Accountability Act includes in its definition of covered entities any person, partnership or corporation, which the FTC has jurisdiction over under Section 5(a)(2) of the FTC Act (15 U.S.C. 45(a)(2)), and as well as those covered entities that had $50,000,000 in average annual revenue for the past three years or ones that possess or control personal information on more than 1,000,000 consumers or 1,000,000 consumer devices.

One of the key requirements proposed by the Accountability Act is **to mandate that covered entities conduct a DPIA under certain circumstances**. A DPIA is defined as "a study evaluating the extent to which an information system protects the privacy and security of personal information the system processes."

The Accountability Act's overall intent is to prevent risk and harm from automated decision systems as to the privacy or security of personal information of consumers. Some of the risks that are mentioned that could potentially negatively impact consumers include violations of privacy and security, inaccuracies, bias and discrimination — which can possibly result from automated decisions.

The bill would require the implementation of "an assessment of the relative benefits and costs of the automated decision system in light of its purpose, taking into account relevant factors, including:

- data minimization practices;

- the duration for which personal information and the results of the automated decision system are stored;
- what information about the automated decision system is available to consumers;
- the extent to which consumers have access to the results of the automated decision system and may correct or object to its results; and
- the recipients of the results of the automated decision system."

To avoid the above-referenced risks to consumers, covered entities are required to implement technological and physical safeguards. Special attention is given to what is defined as a "High-Risk Automated Decision System" or a "High-Risk Information System." These systems are categorized as "high-risk" and can include but are not limited to the following: "the personal information of a significant number of consumers regarding race, color, national origin, political opinions, religion, trade union membership, genetic data, biometric data, health, gender, gender identity, sexuality, sexual orientation, criminal convictions, or arrests."

The Accountability Act states that once enacted, the FTC has up to two years to promulgate regulations in accordance with Section 553 of Title 5, U.S.C. Included in the regulation is a requirement that covered entities would have to conduct a DPIA "of existing high-risk information systems, as frequently as the Commission determines is necessary." The publication of the DPIA is optional, and it is at the sole discretion of the covered entity whether or not to make it public.

In addition, the Accountability Act provides for enforcement by the FTC under unfair or deceptive acts or practices under section 18(a)(1)(B) of the FTC Act (15 U.S.C. 57a(a)(1)(B). However, it also allows state attorney generals to "bring a civil action on behalf of the residents of the State in an appropriate district court of the United States to obtain appropriate relief."

The enforcement net for the Accountability Act has been cast very wide, as it also allows for actions to be brought by other state officials. There is no federal preemption as a result of the Accountability Act, as it clearly states that nothing may be construed in the act to preempt any state law. The message being conveyed to potential covered entities is that they are expected to ensure fairness, impartiality and transparency in their automated decision making, which should provide consumers with enhanced data privacy and protections from algorithmic biases and risks. Over the past several years, there has been a heightened focus on data privacy and protection. All indications point to the fact that this will only increase for the foreseeable future — and on a global level.

ICCR

FEBIS takes part in latest ICCR meeting in Poitiers

Luis Carmona attended the latest ICCR meeting in Poitiers at the beginning of April to represent FEBIS. it was the most attended ICCR meeting with 49 participants. The major issues discussed at ICCR meeting were :

- The implementation in South Africa, as a pilot project, of **the policy guidance** that ICCR published recently on use of alternative data in credit reporting. The doc refers to FEBIS comments, discussed in Washington, on the availability of data needed by our industry. They have considered this in their new legislation on financial systems in relation to credit reporting legislation.
- **The Guidance Policy draft on credit scoring** :
    - Glossary terms are clarified to include definition of CRSP (Credit Reporting Service Provider), as well as CSP (Credit Service Provider) which referred to the suppliers of credits banking sector.
    - This document will include de as “credit grantors” the trade credit lenders “creditors”. Taking into account that they are central banks G20, those who subscribe it, it is very important. It is a crucial term for an important part of our industry and, usually, forgotten by regulators.
    - The draft passed a phase of last reading by members of ICCR and then a period of public consultation from 3 weeks on the website of the IFC and WB. After this procedure, it will become a new publication of the ICCR - World Bank.
    - In the data section: We included a list of essential data that must be present in order to make a proper credit assessment. It shows where each piece of public information is available.
        - Updated financials: not older than 6 months.
        - Shareholders and participations: This Information is available at notaries and public registries.
        - Activity of businesses (companies and sole entrepreneurs) with economic activity: census of new comers, resignations and modifications in the status.
        - Census of company’s non-complaint with social security obligations and/or any payment regularization by the companies with the social security.
        - Census of VAT numbers, of economic agents with current activity, active and non-active, (subject to the tax Authority).
        - Census of companies /entrepreneurs that do not comply with tax obligations.
        - Number of employees subscribed to the social security

- Cooperatives/Other non-registered companies: lack of updated census to be aware of the existence of the entities. Information available at the public administration.
- Judicial information: Judgements' database from civil, mercantile and labour courts.
- Census of companies with transactions abroad
- Official payment performance from the banking industry supervised by central Banks. Nowadays only available for financial entities. Information available at the financial entities' files.

- The paper will now be scrutinized by ICCR secretariat for final version and it will then be made available for final comments to ICCR members. It is a good milestone as FEBIS has been able to include a number of comments in it, showing the importance of being active into ICCR.

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.