MONITORING REPORT
N. 19/2019

efamro
the European Research Federation

IN THIS ISSUE

FACIAL RECOGNITION

THE USE OF BIOMETRIC DATA AND IN PARTICULAR FACIAL RECOGNITION ENTAIL HEIGHTENED RISKS FOR DATA SUBJECTS' RIGHTS.

While the EDPB consultation on Guidelines 3/2019 on processing of personal data through video devices are still open, facial recognition is getting rampant attention.

UK ICO TO PROBE KING'S CROSS FACIAL RECOGNITION

THE INFORMATION COMMISSIONER'S OFFICE (ICO) HAS OPENED AN INVESTIGATION FOLLOWING MEDIA REPORTS ON FACIAL RECOGNITION TECHNOLOGY BEING USED WITHIN SECURITY CAMERAS IN THE KING'S CROSS AREA OF LONDON

The privacy regulator said it was "deeply concerned" about the increasing use of facial recognition technology in public spaces. Under the General Data Protection Regulation (GDPR), facial images are categorised as 'sensitive personal data', which organisations require explicit consent to collect.

The use of facial recognition technology in the area around King's Cross station was first reported by *the Financial Times* on Monday (12th August). Camden Council told the *BBC* it was unaware the technology was being used. Argent, the developer behind the site, has said in a statement it used the tool to "ensure public safety".

The ICO said it would inspect the technology and its operation to see how it is used and whether it complies with data protection law. Denham added: "Any organisations wanting to use facial recognition technology must comply with the law – and they must do so in a fair, transparent and accountable way. They must have documented how and why they believe their use of the technology is legal, proportionate and justified."

Information commissioner Elizabeth Denham said: "*Facial recognition technology is a priority area for the ICO and when necessary, we will not hesitate use our investigative and enforcement powers to protect people's legal rights. "We have launched an investigation following concerns reported in the media regarding the use of live facial recognition in the King's Cross area of central London, which thousands of people pass through every day*."

Katie McQuater for ResearchLive

MANCHESTER CITY WARNED AGAINST USING FACIAL RECOGNITION ON FANS

THE GUARDIAN REPORTS THE CIVIL LIBERTIES ORGANISATIONS COMMENTS ON THE CLUB'S INTENTIONS

Apparently behind the idea is Blink Identity, a Texas-based facial recognition company, says its technology can identify people walking at regular speed, so fans will not need to slow down to show a ticket or use a turnstile. To opt in, supporters would need to register a selfie taken on their phone. Blink Identity says it is also possible to "collect usable and sharable data" on every person that walks through its facial scanning software. The team behind Blink Identity have spent the last decade creating large-scale biometric identification systems in the Middle East for the US Department of Defense, according to its website. Last year Live Nation, the company that owns Ticketmaster, announced investment in Blink Identity as part of plans to replace paper tickets with facial recognition.

The full article available here

CZECH REPUBLIC: UOOU ON USE OF FACIAL RECOGNITION IN FOOTBALL STADIUMS

úřad pro ochranu osobních údajů
the office for personal data protection

THE OFFICE FOR PERSONAL DATA PROTECTION PUBLISHES AN OPINION ON ITS WEBSITE ON THE POSSIBILITIES OF IDENTIFYING AND PREVENTING ACCESS TO FOOTBALL STADIUMS BY UNWANTED PERSONS. THESE ARE PERSONS WHO GROSSLY DISRUPTED THE COURSE OF PREVIOUS MATCHES WITH SERIOUS CONSEQUENCES FOR THE ORGANIZING CLUB, WHO INTENDS TO EXCLUDE THEM FROM VISITING FOOTBALL MATCHES FOR A CERTAIN PERIOD OF TIME.

The documents submitted by the sports club suggested using the *face recognition* technology by the match organizer when entering the stadium. However, as a special category of personal data - biometric data for the unique identification of a natural person, this technology is subject to the conditions of Article 9 of the GDPR on the processing of specific categories of personal data.

This Article requires explicit legal authorization for the processing of biometric data, even if there is a significant public interest, which must be proportionate to the objective pursued, respect the substance of the right to data protection and provide appropriate and specific safeguards to protect the data subject's fundamental rights and interests. The current Act on the Promotion of Sport, which only generally regulates measures to ensure order in the course of a sporting event and the issuance of the Visitors' Rules, cannot be considered as a sufficient power to process biometric data. Neither the Czech Personal Data Processing Act nor any other legal regulation contains such special legislation.

In the current legal situation, therefore, it is not possible to find a sufficient legal reason to process the biometric personal data of football match visitors with *face recognition* technology by the owner of the sports facility as a personal data controller.

Translated by Google. Original version available here

CHATHAM HOUSE
The Royal Institute of International Affairs

THE PROMISE AND PERILS OF FACIAL RECOGNITION TECHNOLOGY

Lyndsey Jefferson speaks to Emily Taylor about the increasing prevalence of facial recognition technology and whether current laws are enough to address privacy concerns.

Chatham House on Medium

AUDIO RECORDING

IRISH DPC QUESTIONS FACEBOOK'S TRANSCRIBING OF AUDIO CHATS

SOCIAL MEDIA GIANT SAYS PEOPLE OPTED IN TO HAVING THEIR CONVERSATIONS RECORDED

Facebook is facing questions from Ireland's data protection watchdog — the agency that oversees the company's privacy standards across the European Union — about why it allowed outside contractors to listen and transcribe people's audio chats through Facebook's platforms.

POLITICO has the full story

HUNGARIAN NATIONAL DATA PROTECTION AND FREEDOM OF INFORMATION AUTHORITY (NAIH) IS INVESTIGATING FACEBOOK'S AUDIO RECORDING PRACTICES

NAIH COMMUNICATION ON VOICE RECORDING PRACTICES BY TECH GIANTS

Facebook must provide written guarantees that it would not disclose the transcripts of users' voice calls to third parties, or else Hungary's data protection authority (NAIH) will ban the service provider from doing so

Hungary wants guarantees that Facebook will not pass on the conversations of its Hungarian users to third parties, an official has said.

On Wednesday, Facebook admitted that it recorded the conversations of the users of its Messenger chat application and made transcripts of those. Facebook, while adding that this happened with the consent of users, said it will cease the practice.

According to *Rmx.news*, Attila Péterfalvi, head of the National Authority for Data Protection and Information Freedom (NAIH), said on Thursday that Hungary will seek written guarantees from Facebook that the transcripts of Hungarian users' conversations will not be passed on to third parties.

Given that Facebook has its European headquarters in Ireland, in the European Union the case will be investigated by the Irish Data Protection Commission, but Péterfalvi added that the Hungarian NAIH will work closely with its Irish counterpart on the matter.

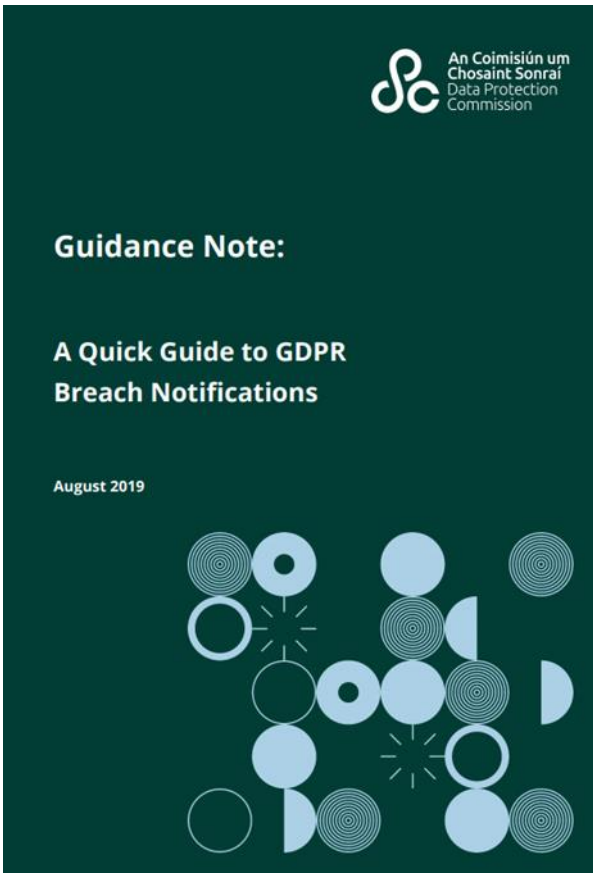
He added that should Facebook's guarantees prove insufficient; Hungary will use the EU's data protection directive GDPR to enforce its demand.

Hungarian constitutional scholar Bernát Török, director of the National University of Public Service's Information Society Research Institute told Magyar Nemzet that while no single national authority has the teeth to effectively take on multinational giants, they can and must enforce national legislation in their own territory.

"Despite many opinions to the contrary, emerging international practice shows that there is such a thing as a 'national online space' within which national authorities and legislators can enforce their will," Török said.

NAIH communication in Hungarian here and news report here

NATIONAL DPAs GUIDANCE



Full guidance available here

IRELAND: DPC PUBLISHES GUIDANCE ON GDPR BREACH NOTIFICATIONS

THIS QUICK GUIDE IS INTENDED PRIMARILY TO HELP CONTROLLERS BETTER UNDERSTAND THEIR OBLIGATIONS REGARDING NOTIFICATION AND COMMUNICATION REQUIREMENTS – COVERING BOTH NOTIFICATION TO THE DPC, BUT ALSO COMMUNICATION TO DATA SUBJECTS, WHERE APPLICABLE.

There are **two primary obligations** on controllers under this regime: **(a)** notification of any personal data breach **to the DPC, unless** they can demonstrate it is **unlikely to result in a risk** to data subjects; and **(b)** communication of that breach **to data subjects**, where the breach is **likely to result in a high risk** to data subjects. It is of utmost importance that controllers understand and comply with both of these obligations.

Controllers must also ensure, in line with the accountability principle set out in Article 5(2) GDPR, as well as the requirements of Article 33(5), that they document any and all personal data breaches, including the facts relating to the personal data breach, its effects and the remedial action(s) taken – this will enable them to demonstrate compliance with the data breach notification regime to the DPC. The DPC also recommends that controllers read the detailed guidance provided on topics including the definition of a personal data breach, assessing risk notification and communication requirements, and accountability, found in the Article 29 Working Party 'guidelines on personal data breach notification'

UK ICO UPDATES GUIDELINES ON SUBJECT ACCESS REQUESTS

The timescale has now changed to reflect the day of receipt as 'day one', as opposed to the day after receipt.

Full updated guidance here

ICO & SAR IN PRACTICE

HUDSON BAY FINANCE LTD ISSUED WITH AN ENFORCEMENT NOTICE FOR FAILING TO RESPOND TO A SUBJECT ACCESS REQUEST.

You can read the press release here and the Notice here

I GOT A SAR ON MONDAY; SEARCHED ACROSS MY FILES ON TUESDAY, EXTENDED THE DEADLINE ON WEDNESDAY; AND ON THURSDAY AND FRIDAY AND SATURDAY; I DISCLOSED ON SUNDAY (AN UPDATED SAR RESPONSE DEADLINE FROM THE ICO)

By Amy Lambert at FieldFisher

Unlike the classic Craig David '00s hit parodied for the purposes of this blog title, the Information Commissioner's Office ("ICO") is thankfully not now suggesting that SAR disclosures should be made outside of the working week. However, the latest updated guidance from the ICO regarding the calculation of the time limit to respond to a subject access request ("SAR") has reduced the amount of time that controllers have to comply with such requests.

Under the General Data Protection Regulation ("GDPR") a subject access request must be dealt with "without undue delay and in any event within one month of receipt of request". In addition, this period may be extended by a further two months where necessary, taking into account the complexity and number of requests. Despite this, the controller must still inform the requestor about the extension within one month of the receipt of the original request (along with the reasons for the delay).

Until recently, the ICO's guidance on responding to SARs stated that the one-month time limit began to run the day after the request was received (or, where the identification of the requestor was reasonably required, the day after the verification of their identity). Or, to put it another way:

- The SAR is received on 12 August 2019. The one-month deadline begins to run on 13 August 2019. Unless extended, the response deadline is 13 September 2019.

This is now no longer the case.

The latest version of the ICO's guidance has stated that, in contrast to previous guidance, the deadline for response now starts running on the day that the request is received (or, the date that the requested verification is received).
The rest of the ICO guidance for calculating SAR response timelines remains as it was.
For example, if the following calendar month is shorter (so there is no corresponding calendar date), the ICO's position remains that the date for the response must be the last day of the following month. For example:

- The SAR is received on 31 March 2019. - The one-month deadline begins to run on 31 March 2019. - Unless extended, the response deadline is 31 April 2019, which does not exist. - The deadline for response is therefore 30 April 2019.

In addition, the ICO has made it clear that (helpfully) if the corresponding date falls on a weekend or a public holiday, the controller still has until the next working day to respond. For example:

- The SAR is received on 14 August 2019. - The one-month deadline begins to run on 14 August 2019. - Unless extended, the response deadline is 14 September 2019, which is a Saturday.
- The deadline for response is therefore 16 September 2019 (a Monday, the next working day).

As ever, the ICO also suggests that if businesses need to implement a standard response period for any and all SARs received, for practical purposes it may be useful to adopt a standard 28-day period for responding, to ensure that the controller always complied within a calendar month.
However, for those living SAR deadline to deadline, time to recalibrate those timelines.

ENFORCEMENT

ENFORCEMENT UNDER THE GDPR – THE NEW PARADIGM

BEFORE THE GDPR CAME INTO EFFECT, ORGANISATIONS WERE UNDERSTANDABLY APPREHENSIVE ABOUT THE EXPONENTIAL INCREASE IN POTENTIAL FINES UNDER THE NEW REGIME

During 2018, the level of fines seen did not represent a significant increase on pre-GDPR fines for breach of data protection laws. However, the landscape has now significantly changed with a number of multi-million pound fines demonstrating regulators' willingness to use their new enforcement powers.

Barry Fishley and Muzaffar Shah of Weil Gotshal & Manges LLP analyze the major fines here

LITHUANIA: THE STATE DATA PROTECTION INSPECTORATE PUBLISHES STATISTICS ON COMPLAINTS

GENERAL DATA PROTECTION REGULATION. THE RIGHT OF ACCESS TO YOUR PERSONAL DATA IS PROTECTED

In 2019 about **7 percent** of the **complaints** received by the State Data Protection Inspectorate (SSIA) consist of individuals' rights complaints. Most people seek justice for the right to be forgotten, to object to data processing, and most often for the **right to access data**. It was because of the improper implementation of this right that the SDPI imposed the first **fine** (EUR 2,395) on the municipal enterprise. In 2019, this decision of the SSIA August 8 has already been approved by the Vilnius Regional Administrative Court.

In this case, the fine was imposed because the person approached the company to access his personal data processed by that company, but the company did not properly enforce this right. First of all, in its reply, it did not specify **specific data**, but only what type of personal data it processes. The company did not meet the deadline for replying and responded more than six months instead of **1 month**. In particular, the company provided an erroneous reply as it **did not provide all** but some of the data.

Although the right of access is enshrined in BDAR, it is not a new right. Under Lithuanian legislation prior to the BDAR, organizations were required to enforce this right earlier, but in some cases, there is often a lack of knowledge on how to properly enforce it.

The SDPI points out that every person has the right to obtain from the organization confirmation that he or she is processing personal data relating to him or her. Requests may be made orally or in writing, with the appropriate proof of identity. In the event of processing, the individual shall have the right of access to his or her data and shall have access to the following information:
- For what **purposes** ;
- **Who** was (or will be) **disclosed** ;
- Expected retention **period** ;
- the **right to** rectify, delete, restrict or refuse such processing;
- The right to lodge a **complaint to the** supervisory authority - the SSIA;
- When information is not collected from you, to obtain information on the **sources** of the data ;
- The existence of **automated decision-making** , including profiling, and information about its rationale, as well as the significance and foreseeable consequences for you of such processing;
- The transfer of data to a third country or an international organization and appropriate safeguards regarding transfer.

Translation by Google. You can read the press release here and the FAQs here, both only available in Lithuanian

THE BUSINESS OF DATA

JANE BAINBRIDGE REPORTS.

With increased focus on the ethics around how companies are collecting and using personal data, some members of the Market Research Society's Delphi Group took part in a roundtable discussion on what business needs to do.

Jane Bainbridge for IMPACT MAGAZINE


efamro