Márton Domokos Senior Counsel, Co-ordinator of CEE Data Protection Practice
marton.domokos@cms-cmno.com

CMS Cameron McKenna Nabarro Olswang LLP Magyarországi Fióktelepe, Budapest

Valentina Parvu Senior Associate
valentina.parvu@cms-cmno.com

CMS Cameron McKenna Nabarro Olswang LLP, Bucharest

Ksenija Ivetić Marlović Senior Attorney
ksenija.ivetic@cms-rrh.com

Petrikić & Partneri AOD, Belgrade

Andrea Cervenkova Associate
andrea.cervenkova@cms-cmno.com

CMS Cameron McKenna Nabarro Olswang, advokáti, v.o.s., Czech Republic

Angelika Sedlackova Senior Associate
angelika.sedlackova@cms-cmno.com

CMS Cameron McKenna Nabarro Olswang LLP, Bulgaria

Martina Novysedlakova Associate
martina.novysedlakova@cms-cmno.com

CMS Cameron McKenna Nabarro Olswang, Slovakia

Central and Eastern Europe round-up: enforcement decisions and major developments

When planning business operations in Central and Eastern Europe ('CEE'), data protection law is as important as any other area of law. Most business projects will involve some processing of personal data, whether that of employees, customers or potential clients. In fact, personal data protection rules will potentially apply in any scenario where information relating to an individual is involved in any way. Although the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') is harmonising the data protection laws also in the CEE, local laws will continue to apply, e.g. in employment-related data processing, cybersecurity, and cookie compliance. Angelika Sedlackova, Andrea Cervenkova, Márton Domokos, Valentina Parvu, Ksenija Ivetić Marlović and Martina Novysedlakova from CMS Cameron McKenna Nabarro Olswang, discuss the most relevant enforcement decisions and developments that have recently taken place in Bulgaria, the Czech Republic, Hungary, Romania, Serbia and Slovakia, and which must be taken into account by companies operating in such jurisdictions.

Bulgaria

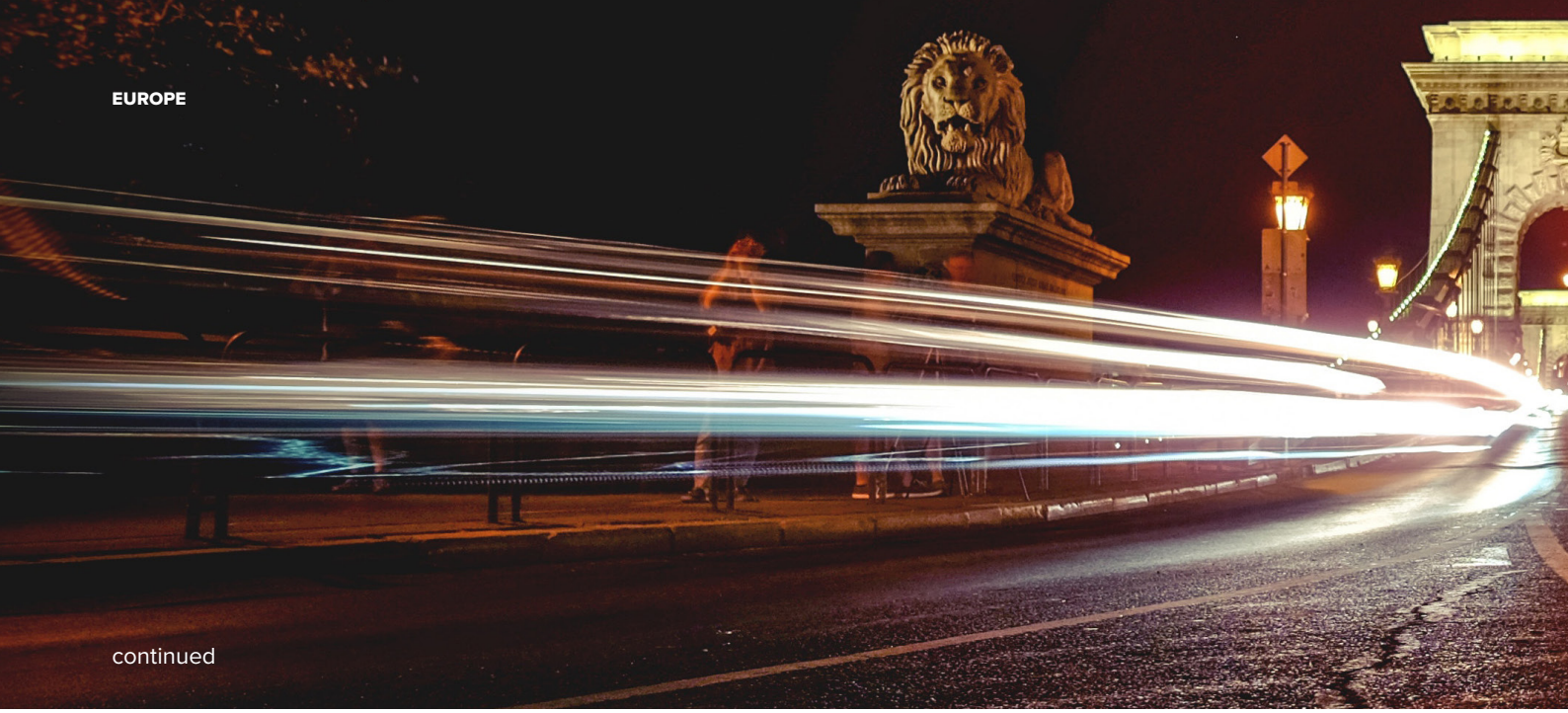
For the first time since its creation, in 2016, the Commission for Personal Data Protection ('CPDP') conducted a comprehensive sector compliance examination, which concerned the education sector and included 4,611 educational institutions of various kinds. Among other mandatory instructions to the monitored educational institutions, the CPDP expressly prohibited kindergartens to request and store copies of birth certificates of applicant children.

In addition, a number of verifications were executed by the CPDP at the end of 2016 regarding presidential elections and a national referendum, both held in November 2016. The subject of concern was the processing of personal data by political parties and coalitions gathered via signature subscriptions. Six parties, three coalitions and 12 initiative committees were sanctioned for processing personal data without proper registration with the CPDP. Further, at the end of 2016, the CPDP issued its decision in a case related to personal data processed by the National Revenue Agency ('NRA'). The CPDP established that, when it revealed personal data of an individual subject to a NRA verification to third parties and in notifications addressed to them for collection of documents, the NRA violated the prohibition to conduct additional processing in a manner incompatible with the purpose of processing. The NRA was sanctioned with BGN 10,000 (approx. €5,110).

In March 2016, the CPDP addressed a case related to the powers of private bailiffs in Bulgaria. A well-known private bailiff in Sofia was imposed a pecuniary sanction of BGN 10,000 for the following violation: he processed personal data of an individual who participated in the enforcement case in his capacity as a mortgage (not main) debtor. The CPDP ruled that under the enforcement procedure a mortgage debtor participates to the extent that enforcement actions may be initiated towards the mortgaged real estate, not only towards the mortgage debtor himself. Gathering data for the economic status of the mortgaged debtor was found illegal.

A recent media case saw the CPDP imposing a sanction of BGN 15,000 (approx. €7,670) to the owner of a news oriented internet site for publishing a politician's personal data. The defendant based its arguments on the freedom of speech and information of society principles. Nevertheless the CPDP ruled that said principles would not be violated if sensitive personal data was properly deleted.

Another interesting case related to a company providing test drive services, which required to be presented with copies of identity cards and driving licences of its customers. The CPDP



continued

ruled that the requirement for a driving licence corresponded to the provided service, but the requirement to provide the identity card was incompatible with the purpose of processing. The test drive company was sanctioned with BGN 12,000 (approx. €6,130).

The highest sanction imposed by the CPDP amounted to BGN 63,000 (approx. €32,210) and was imposed to Sofia Water Supply company for providing personal data of its customers to a debt collecting company without proper prior consent.

Czech Republic

Unsecured client personal information stolen by an employee

The Office for Personal Data Protection of the Czech Republic ('UOOU') issued a fine of CZK 3,600,000 (€144,000) to T-Mobile Czech Republic for the theft of client personal data by a T-Mobile employee. The UOOU held T-Mobile was responsible for not having the personal data of clients within its electronic database properly secured. The stolen data included names, dates of birth, bank accounts and information on telephone plans or average spending. The former employee was also being prosecuted criminally.

Highest fine for spam

The highest data protection penalty issued in 2017 was a fine of CZK 4,250,000 (€170,000) to EURYDIKAPOL, s. r. o. (also known as JH HOLDING s. r. o.). This has also been the highest fine issued so far for unsolicited commercial messages. The spam was sent out repeatedly over a year, with the company being unable to prove consent of the receivers to such messages. The fact that the company continued the unlawful practice even during the investigation, as well as the large amount of messages (in one case a receiver was sent nearly 200 messages) sent was partially the reason for the amount of the fine.

Posting a picture of a shoplifter on Facebook

The UOOU published an official statement after the Czech Constitutional Court ruled on the infamous case of the company ekolo.cz sro. In this case, an electric bicycle was stolen by a shoplifter, who was recorded by a security camera in the shop. When police were unable to find the offender even when provided with a clear picture of him as recorded by the camera, the shop owner published the photograph on Facebook asking the public for help. As the status went viral, with help of the public, the shoplifter was identified, caught by police and criminally prosecuted.

However, the UOOU fined the shop owner for violating the rights of the later convicted shoplifter by posting his picture on Facebook. While this legal opinion has been approved by the courts of appeal and by the Constitutional Court, the UOOU itself, with its new director, later stated this would not have been opined, and that such a strictly formal application of law is unjust.

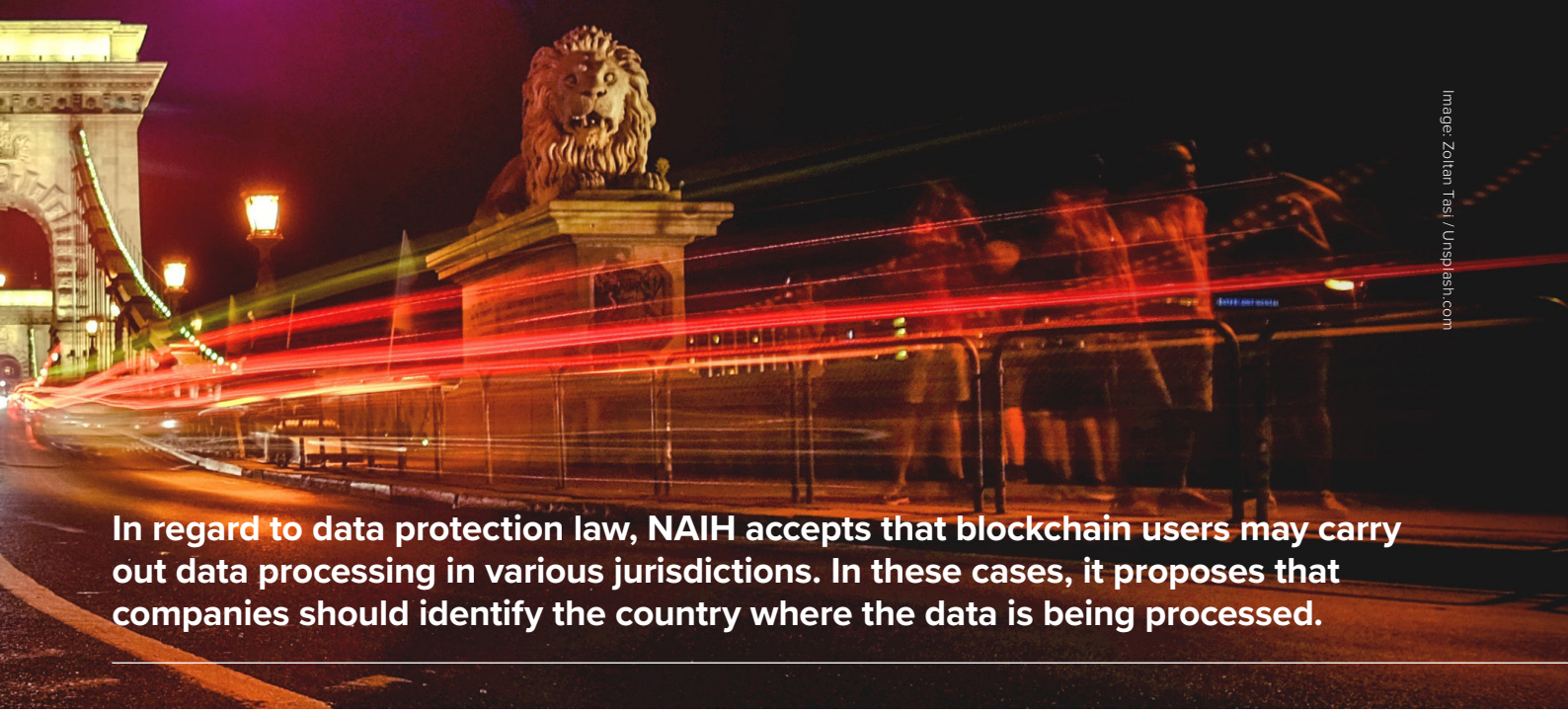
Hungary

Copying IDs, form of consent and contacting the customers' employer

In Hungary, the National Authority for Data Protection and Freedom of Information ('NAIH'), imposed a HIF 1,000,000 fine (approx. €3,200) on a company whose business was selling and managing a wide range of financial services, including consumer credit, payment solutions, loan redemption and banking services. Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information ('the Info Act') provides that companies can process personal data only for specified and explicit purposes, where it is necessary for the implementation of certain rights or obligations.

The purpose of processing must be satisfied in all stages of data processing operations; recording of personal data shall be done under the principle of lawfulness and fairness. The NAIH declared that individuals shall provide personal data only if such data are necessary for concluding, performing or terminating the financial services agreements, and it is the financial services provider who shall prove that these criteria are fulfilled. The NAIH found that making copies of ID cards of customers who appeared at the financial service provider in person is excessive, even if the customers provide their prior consent to such practices. The NAIH argued that the financial service provider shall identify the customer once he/she has shown the ID, and that it is not necessary to make and store a copy of it as well, since a copy will not have any probative force (compared to the original document).

The NAIH also reviewed other consent forms used by the company and found that it was not enough to indicate 'direct marketing' as a data processing purpose: the privacy information notice provided should contain the exact use of such data, including marketing as well. Moreover, the NAIH claimed that it may be enough to use anonymised information for product development statistics, and such purpose does not require the use of the actual personal data of customers.



In regard to data protection law, NAIH accepts that blockchain users may carry out data processing in various jurisdictions. In these cases, it proposes that companies should identify the country where the data is being processed.

As regards the verification of customers' income, the NAIH declared that the financial services provider could contact the customer's employer only upon the prior - preferably written - consent of the customer. The customer shall provide his/her consent separately for each data processing purpose, and the privacy notice shall specify the list of personal data that the financial services provider can process. It is unlawful if the privacy notice states that the financial services provider can obtain any personal data from the customer's employer or other bank.

Prize draw competitions and personal data

Further, the NAIH imposed a HIF 1,000,000 fine (approx. €3,200) on an insurance company who offered a prize draw competition for its customers without providing adequate privacy information. For example, the NAIH found that the privacy notice pertaining to the competition did not contain a detailed list of the data processors involved, including their specific activity and for how long they could access the participants' data. The NAIH also looked into the mandatory registration of the company in the Data Protection Registry and found that the content of the registration did not match the information provided in the privacy notice in many respects, such as the scope of data, the processing purpose and the data retention period. The privacy notice did not contain detailed information on the participants' data protection rights and remedies either, e.g. the deadlines applicable for the company to fulfil the individuals' requests, and indication of the competent court. The NAIH also ordered the insurance company to obtain a separate consent for the transfer of personal data to another member in its company group (who would send marketing messages) and conclude a data transfer agreement for this purpose. The insurance company was required to publish the privacy notice on its website.

Data protection aspects of blockchain

Recently, the NAIH issued guidance on blockchain and data protection. The guidance answers the questions of a private individual in a specific case, and the NAIH published it due to public interest and the rise of the technology. The guidance provides a short description of blockchain technology, defines personal data, the legal bases of data processing, and how to identify the data controller and data processor in the blockchain.

According to the NAIH, blockchain is a decentralised network where no central entity controls system functions and transactions executed with the data. Each user is engaged in data processing, and each person who adds blocks and personal data to blocks in the system is a data controller. Subsequent users may later add personal data to the system and obtain an exclusive right to dispose of their data stored in blocks. In this case, they can execute a transaction using the data. As a result of a transaction, if the right to dispose of personal data stored in the block is transferred to another user (i.e. the recipient of data who will have the exclusive right of disposal), the NAIH considers this user a data controller.

While it provides practical guidance on how to identify the data controllers and data processors in the blockchain, the NAIH does not address how FinTech companies can follow this approach in the case of a large blockchain, and in particular compliance with Privacy by Design obligations. Moreover, the NAIH does not go into detail about technical solutions (e.g. data access management platforms) to address the complex obligations of FinTech companies to demonstrate that they are compliant when processing data in the blockchain.

In regard to data protection law, the NAIH accepts that blockchain users may carry out data processing under various jurisdictions. In these cases, it proposes that companies should identify the country where the data is being processed. This would be the country where the data controller is carrying out the actual data processing operations. (i.e. where he/she places a transfer order, accesses and adds data to the blockchain, mines bitcoin, or issues orders to carry out operations). The NAIH confirms that the physical location of the data in the blockchain is irrelevant, but states that the Court of Justice of the European Union ('CJEU') approach in the *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (C-131/12) would also apply. While the examples provided by the NAIH are a good starting point for FinTech companies to determine what laws are applicable to their operations, the GDPR will also have a major impact on the industry.

Regarding the question whether the long-term use of blockchain makes users and their patterns of behaviour vulnerable to monitoring and profiling, the NAIH states this risk depends on the characteristics of a specific

Serbia has been waiting for the new personal data protection law for over two years. Personal data protection is one of the topics of chapters 23 and 24 of Serbia's accession negotiations with the EU.

continued

system, the data processed in it, and its auxiliary data processing operations.

In conclusion, the NAIH guidance is highly important since Hungary has a dynamic privacy-sensitive FinTech scene. The NAIH touches key points of the data protection obligations of companies, but it is clear that market players and users expect more detailed sector-specific guidance in the following areas: Privacy by Design, subject access rights, data retention, data reversibility, data security, and transparency obligations.

Romania

In anticipation of the entry into force of the GDPR, the Romanian Ministry of Internal Affairs launched, on 5 September 2017, for public debate, a bill for the amendment of the current legislation on the organisation of the National Supervisory Authority for Personal Data Processing ('ANSPDCP') and for the abrogation of the current Law No. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data.
The main purpose of the draft legislation is to enhance the administrative and institutional capacity of the ANSPDCP (currently considerably under-staffed and under-budgeted) so that the ANSPDCP can effectively cope with its role and new attributions of control and safeguard of the rights of the EU citizens, as enriched in the GDPR.

The draft legislation also aims to set out a unitary and detailed framework for the performance by the ANSPDCP of its powers of control, in particular with regard to the conduct of investigations and the solving of complaints.

The following are worth mentioning:

- The ANSPDCP is entrusted with large powers of control of data controllers and their empowered persons, including via impromptu investigations, request of information, witness interviews, and access to the locations and the equipment where data is stored (note: the ANSPDCP would need a court approval to conduct such investigations only in the situation that the personnel entrusted with the control mission would encounter obstacles from those investigated).
- The actions available to the ANSPDCP to ensure compliance are classified as 'corrective measures,' recommendations and cease orders by the courts (in the latter case, the data subject automatically becoming a plaintiff). The corrective measures include administrative sanctions (i.e. fines and warnings; other measures include prohibition of processing, erasure of the data, suspension of data flow towards a third country).
- There is a proposed threshold of €300,000 as a fine, above which the attribution to apply the fine rests exclusively with the President of the ANSPDCP (also, if a fine larger than the RON equivalent of €300,000 is being considered, the ANSPDCP is required to issue, in addition to minutes of the investigation, an investigation report, which normally includes significantly more information than the minutes, and is comprehensive of the defence of the controlled entity).
- Note, the fine is to be paid within a term of 15 days (the position of the ANSPDCP's representative as further reflected in the draft legislation is that the right - under the common administrative contentious rules - to pay half of the amount of an administrative fine if payment is made within 24 hours from the sanctioning would not apply in this context).
- The data controller/empowered person is entitled to challenge the relevant administrative deed of the ANSPDCP before the competent tribunal within 15 days from communication, with the possibility to further appeal the tribunal's decision before the Court of Appeal (no term is provided so far). Note, the challenge does only suspend the payment of the fine, not the other measures that may have been imposed.

Serbia

Serbia has been waiting for its new personal data protection law for over two years. Personal data protection is one of the topics of chapters 23 and 24 of Serbia's accession negotiations with the EU. Earlier this year, the Commissioner for Information of Public Importance and Personal Data Protection prepared a draft law ('the Draft Law'), which was put to public debate. Following the debate and finalisation of the wording of the Draft Law, this was forwarded to the Ministry of Justice for further action. On 14 November 2017, the Minister of Justice Ms Nela Kuburović announced that the Draft Law will soon be available for public debate. However, at the time of publication, the Draft Law is still not publicly available.

Slovakia

The Office for Personal Data Protection of the Slovak Republic ('PDP') does not regularly publish statements or comments on specific cases once an investigation is completed. Instead, it publishes bi-annual reports providing statements on a number of selected significant cases.
In 2016, the highest fine issued by the PDP was €7,000 (whereas the average fine was €2,130) for collecting biometric information without a reasonable purpose. However, detailed information on the case has not been disclosed.

The PDP also investigated an employer who installed GPS tracking devices into cars employees were using, not only for business purposes, but also during their spare time as a form of fringe benefit. During the investigation, it was made clear that the employer was gathering information on location and movement of the employees outside working hours, for which there was no legal reason to do so and thus such behaviour was considered unlawful. No fine was issued as the employer ceased the practice upon notice by the PDP.