

Your World First

C/M/S/

Law . Tax

Happy birthday GDPR in CEE

Overview of the past 12 months – Bulgaria, Croatia,
Czech Republic, Hungary, Poland, Romania, Russia,
Slovakia, Slovenia, Turkey, Ukraine

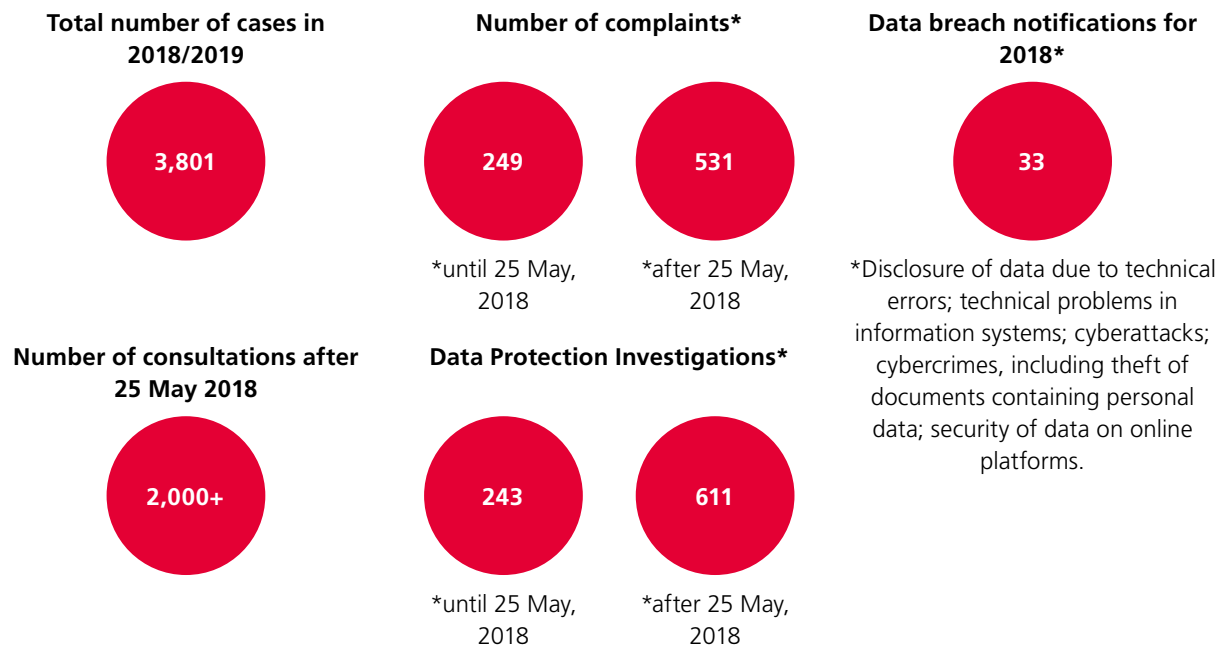
May 2019



Bulgaria

Bulgarian Personal Data Protection Commission (Комисия за защита на личните данни – “PDPC”)

Facts & figures



Watch out for

- specific local rules on background checks, photocopying of official documents, employee monitoring, CCTV operations and entry systems, whistleblowing system, health data, genetic data, anti-money laundering measures.
- companies should revise data processing operations which are necessary for compliance with a legal obligation at least every three years.
- “Opt-in” system for electronic direct marketing advertisements.



Other specific guidance from the regulator

- Information on recipients or categories of recipients of personal data.
- Cookie consent and information.
- Biometric access control systems in the workplace.
- Photographs and video recordings.



The regulator’s list on mandatory data protection impact assessments

- Large-scale and regular processing of biometric data for unique identification of individuals.
- Processing of genetic data for profiling, which produces legal consequences for the individuals or similarly affects them to a significant extent.
- Processing of location data for profiling which produces legal consequences for the individuals or similarly affects them to a significant extent.



- Large-scale processing where a company cannot provide the mandatory data protection notice, or it requires disproportionate effort or seriously hinders processing or is likely to make it impossible.
- Processing of personal data by a data controller whose principle place of establishment is outside the EU, and when its representative in the EU is located on the territory of the Republic of Bulgaria.
- Regular and systematic data processing, where communicating any rectification or erasure of data, or restriction of processing to each recipient proves impossible or involves disproportionate effort.
- Processing of personal data of children in the direct provision of information society services.
- Implementing data migration from existing to new technologies in case of large-scale processing.

Notable cases and takeaways

What happened?	Takeaways...
EUR 27,098 fine for unlawful use of personal data. A customer allegedly requested switching from a subscription to a pre-paid service at a telco. However, it was not the customer who signed the request form – the signature was falsified. As a result, the company processed the underlying personal data for a purpose, which the customer has not consented to. The customer was not aware of this use and did not have the option to consent.	Companies should choose the legal basis for data processing carefully, duly inform the individuals of the data processing terms, and strictly follow their internal data protection policies.
EUR 1,278 fine for carrying out background checks on the employment and insurance status of an ex-employee without legitimate basis.	Companies should restrain from processing ex-employees’ data without legal basis.
EUR 256 fine to an on-line newspaper for publishing a copy of a contract that contains personal data of executive directors of companies (even if the data is available from the Bulgarian Commercial Register).	Companies should be careful when using personal data for purposes different from the one for which the data has been collected and without legal grounds. In such cases, the personal data should be anonymised when publishing documents.
Warning for data processing for a new purpose. The individual was acting as a proxy of a client of the bank, to receive a statement of outstanding contributions and their repayment. The bank also used the personal data included in the POA to register a new client file for the proxy, although this was not the purpose for providing the proxy’s personal data.	Companies must ensure that they are processing personal data only for the specified purposes and legal grounds and no additional processing of data is carried out without being justified. Individuals must be informed on data processing purposes.

For further information, please contact:



Angelika Sedlackova
Senior Associate
T +359 2 923 4851
E angelika.sedlackova@cms-cmno.com



Tatyana Yosifova
Junior Associate
T +359 2 923 4852
E tatyana.yosifova@cms-cmno.com

Croatia

Croatian Personal Data Protection Agency (Agencija za zaštitu osobnih podataka – “AZOP”)

Facts & figures

Total number of cases: data for 2018 are not publicly available yet.

Watch out for

- Specific local rules on CCTV operations and employee monitoring, genetic data, biometric data, child consent, data processing for statistical purposes.
- Other specific local data protection rules, especially employment laws, whistleblowing law, anti-money laundering laws, banking laws.
- Individual administrative fines for responsible/authorised persons of the controller/processor related to unlawful use of CCTV recordings (up to HRK 50,000.00 - approximately EUR 6,700.00).
- Possibility of unannounced audits by AZOP.

Other specific guidance from the regulator

- Data processing for marketing and for business purposes.
- Use and suggested form of non-disclosure statement.
- Obligations of controllers and processors, obligations of data protection officers.
- Maintaining records of processing activities.
- Consent as a legal basis (employee’s consent, child’s consent).

The regulator’s list on mandatory data protection impact assessments

- Processing of data for the purpose of systematic and extensive profiling or automated-decision making to make conclusions which significantly affect or may affect an individual and/or more persons, or which are used as tool in decision-making on someone’s access to service, servicing or benefit (e.g. data processing related to economic or financial situation, health, personal preferences or interests, reliability or behaviour, location data, etc.).
- Processing of sensitive data for the purposes of profiling or automated-decision making.
- Processing of children’s data for the purposes of profiling or automated-decision making, for marketing purposes, or for direct service offerings.
- Processing of data collected by third parties when such data is used for the purposes of making decisions on execution, termination, refusal or extension of service agreements.
- Large-scale processing of sensitive data and data relating to criminal/misdemeanour liability.
- Systematic monitoring of public areas on a large scale; use of new technologies or technological solutions (e.g. application of IoT, smart TVs, smart home appliances, etc.) for the purpose of analysing or predicting economic situation, health, personal preferences or interests, reliability or behaviour, location or movement data.
- Processing of genetic or biometric data, when at least one additional condition from the WP29 Guidelines on Data Protection Impact Assessment is fulfilled.
- Connecting, comparing or similarity checking of data from various sources.



- Location/behaviour tracking in the case of systematic processing of communication data (metadata) originating from the use of telephone/internet/other communications (e.g. GSM, GPS, WiFi).
- Use of devices and technologies where a personal data breach may jeopardise health.
- Employee monitoring by use of applications or monitoring systems (e.g. work, location, communication monitoring).

Notable cases and takeaways

What happened?	Takeaways...
Content of records of processing activities: must be elaborated (e.g. detailed description of purposes, retention periods with references to statutory provisions (where applicable) etc.	Companies should revise their records of processing activities to ensure that relevant categories are sufficiently elaborated.
Mandatory records of processing activities – examples when controllers having less than 250 employees meet the criteria: use of new technologies such as biometric readers/face recognition; use of IT services; processing of data for wage payment purposes.	Regardless of the number of employees, it is advisable to keep the records of processing activities whenever employee data are processed by a company and IT services used.
Marketing – legal basis for e-communications (e.g. newsletters): consent or legitimate interest as defined by the Croatian Electronic Communication Act (ECA).	If relying on legitimate interest for newsletters, companies must ensure that they meet strict requirements of the ECA (direct client relationship; similar products / services).
DPOs and conflict of interest: identification of incompatible functions, specific internal rules, precise and detailed contract terms, statements on non-existence of conflict, and specific protective measures should be used.	Companies should revise their existing rules, agreements and measures to ensure their DPOs are not conflicted.
DPO’s contact details: mailing address, phone number and/or email address should be published; name is not mandatory (controller/processor and a DPO to decide); advisable to inform employees of contact details and name.	Companies should ensure their privacy notices, intranet, etc. contain DPO’s contact details.
Employees’ non-disclosure statements: although not mandatory, it is advisable that employees engaged in data processing execute such statements as an organisational measure (to ensure security).	It is advisable to have non-disclosure/ confidentiality statements of/agreements with company’s employees engaged in data processing.

For further information, please contact:



Marija Zrno
Partner
T +385 1 4825 606
E marija.zrno@bmslegal.hr

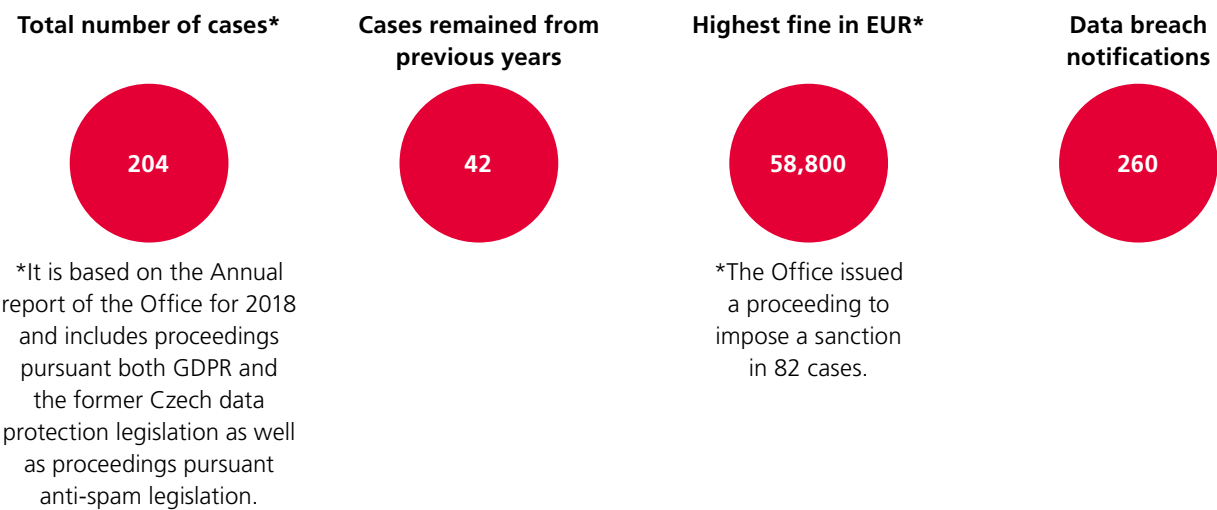


Alina Skiljic
Associate
T +385 1 4825 600
E alina.skiljic@bmslegal.hr

Czech Republic

Office for Personal Data Protection (<https://www.uouu.cz/>) ("Office")

Facts & figures



Watch out for

- Specific local rules on age limit for consent in relation to information society services and retention of CCTV records.
- Exception from general opt-in system for electronic direct marketing advertisements, which allows sending direct marketing messages to the clients regarding the provision of similar services or sales of similar products, provided that the client has a right to easily opt-out.

The regulator's list on mandatory data protection impact assessments

- Monitoring of individuals, particularly using location tracking with coordinates.
- Processing of data of highly personal nature (communication details such as data regarding calls or emails, personal financial data) and special categories of personal data (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or a person's sex life or sexual orientation).
- Processing of data, based on which subjects could be perceived as members of a particular group of people and be endangered as a result (people with criminal history, of a specific religion, sexual orientation or nationality etc.).
- Large-scale data processing (more than 10,000 subjects, more than 20 people having access to such data on behalf of the data controller, more than 20 places where data are processed etc.).
- Monitoring of public places (particularly large-scale CCTV monitoring of public places).
- Processing of data, where individuals have a limited option to influence.
- Processing of publicly available data (typically as a result of a legal obligation of the data controller to make such data publicly available).
- Data processing using technologically advanced platforms (particularly profiling, analysis using artificial intelligence, etc.).

- Processing of data with linkage/relation to other controllers or processors (public authorities, members of entrepreneurial groups, hospitals etc.), mainly where all such controllers or processors cannot be identified.
- Data processing using new technological methods with no previous experience with such methods so far.

The Czech Data Protection Act was published (Act No. 110/2019, "Act")

- In April 2019 the newly adopted Act came into force, introducing some local derogations from GDPR. Among the most commercially relevant ones is the minimum age for a valid consent for data processing, which is being set to 15 years.
- Moreover, the Act encompasses provisions regarding the Office and the prohibition on imposing fines to public administration authorities. Inequality between public and private entities will thus be significant in this respect. Furthermore, journalists, artists and academics are subject to less regulation when it comes to obligations arising out of the GDPR (e.g. information obligation).

Notable cases and takeaways

What happened?	Takeaways...
A company running a private register of entrepreneurs (online commercial and trade register) has been held accountable for breaching GDPR. The website operator failed to comply with an obligation on accuracy of the data processed. (The website operator had no legal title for processing data with respect to entrepreneurs whose trade license expired in the past four years.)	Companies must always ensure in day-to-day operations that the personal data they are processing are accurate and up to date. Companies must also take every reasonable step to ensure that inaccurate data are erased or corrected without delay.
A fine of EUR 58,800 has been imposed on the company Internet Mall, a.s. (operator of a large e-commerce store). The breach lied in failure to secure and prevent a large leak of customer personal data onto a public cloud service Uložto.cz. The fine is exceptionally high compared to other sanctions usually imposed by the Office and it remains clear that the large scale of the breach and data concerned have been considered.	Companies should revise data security and breach management processes.
Login information to electronic documentation of hospital patients has been found insufficient in terms of tracking who has been accessing the documentation. Furthermore, the fact that all doctors had access to almost all documentation on every patient was found too extensive. A fine of EUR 1,500 was imposed as a result.	Companies should revise the level of access to personal data granted to each employee, keep this access as minimal as possible (only where necessary) and provide each employee with a unique login to be able to track who access data and when it is accessed.

For further information, please contact:



Tomáš Matějovský
Partner
T +420 296 798 852
E tomas.matejovsky@cms-cmno.com

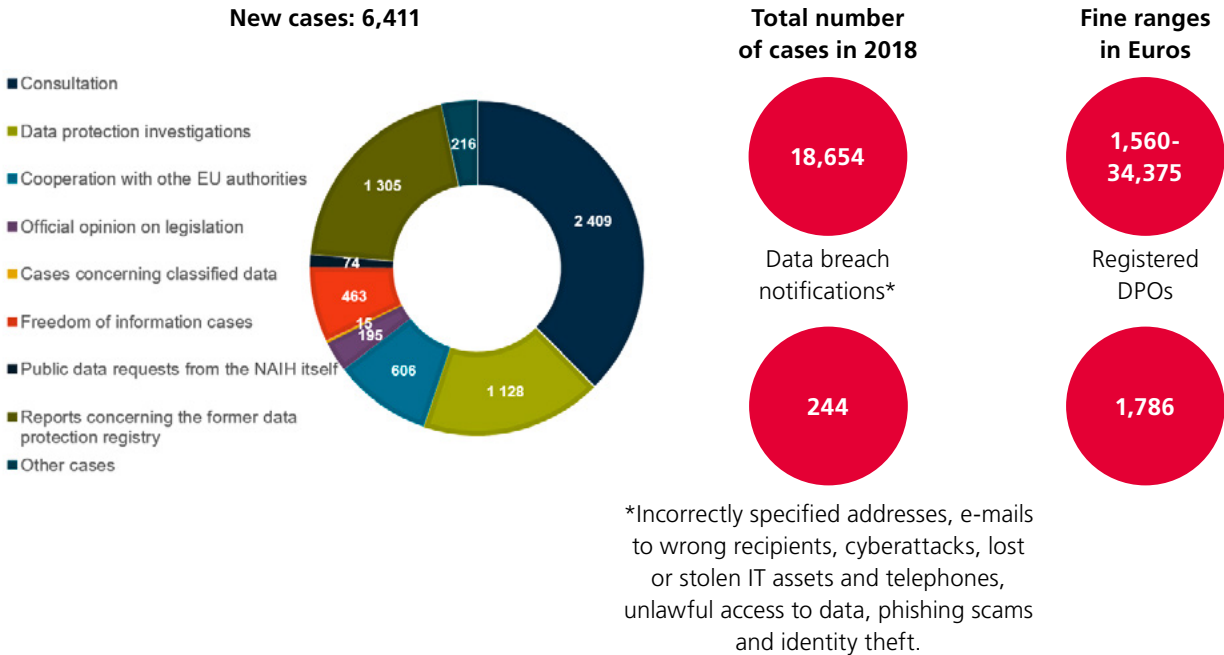


Andrea Červenková
Associate
T +420 296 798 856
E andrea.cervenkova@cms-cmno.com

Hungary

Hungarian Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság – “**NAIH**”)

Facts & figures



Watch out for

- Specific local rules on background checks, photocopying of official documents, employee monitoring, CCTV operations and entry systems, whistleblowing systems, health data, genetic data, anti-money laundering measures.
- Mandatory revision of data processing operations which are necessary for compliance with a legal obligation at least every three years.
- “Opt-in” system for electronic direct marketing messages.

Other specific guidance from the regulator

- Information on recipients or categories of recipients of personal data.
- Cookie consent and information.
- Biometric access control systems in the workplace.
- Photographs and video recordings.

The regulator’s list on mandatory data protection impact assessments

- Healthcare and medical sector, and biometric and genetic data on a large scale.
- Location tracking technologies, the monitoring of public areas (e.g. Wi-Fi tracking, drones).
- Employee monitoring (e.g. GPS or cameras to prevent theft and fraud, cameras and software monitoring keyboard usage, screenshots, mouse movement and e-mail traffic).
- Marketing services (e.g. behavioural marketing, profiling, data collection from multiple sources).
- Services and products for children.


Notable cases and takeaways

What happened?	Takeaways...
EUR 3,135 fine (6.5% of turnover) in case of a CCTV footage access request.	Revise subject access rights (SAR) procedures, do not ask for justification from the individuals.
EUR 1,560 for sending SMS on a credit card debt to the wrong person and refusing to delete the data	Ensure that the processed personal data is accurate and up to date. Restrict data processing until data accuracy is verified. Ask individuals regularly to report any changes.
Warning for using a private person’s tax ID as a general client identification code.	Revise client identification methods and process tax IDs only for tax purposes.
EUR 1,560 fine for failing to include the terms of backup copies in a privacy policy.	Disclose the processing of backup copies in privacy policies.
EUR 3,115 fine for the unlawful disclosure of a whistleblower’s name to his employer, which resulted in the termination of his employment.	Revise the internal processes for answering external data requests.
EUR 3,115 fine for an unsatisfactory legitimate interest balancing test and collecting telephone numbers for claim enforcement.	Balancing tests must be specific, cover only one processing purpose, and prove the priority of the company’s interests over the individuals’.
EUR 34,375 fine for a data breach (cyberattack). A hacker disclosed information on the vulnerability of the organisation’s system and the command used for the attack. The disclosure of the identification data of more than 6,000 users (e.g. names, emails, user names, passwords) posed a high risk.	Revise breach management procedures and data security requirements. Password complexity validation algorithms, which suggest password length and special characters is a must. The encryption technology must contain sufficient levels of protection against malicious decryption techniques.
Warning for a data breach (unlawful access). A journalist using an online vehicle information platform, accessing data such as the manufacturing year, mileage, and engine type of cars, discovered that users were also able to access the personal data of 11,000 people.	The company involved must notify all affected individuals of the breach and advise them to delete any personal data that was unlawfully accessed. Technical photos must not contain unnecessary image of individuals. Recommended mitigation: modified data access settings, internal guidance for employees, e-mail hotline for complaints.

For further information, please contact:

 **Dora Petranyi**
CEE Managing Director
T +36 1 483 4820
E dora.petranyi@cms-cmno.com

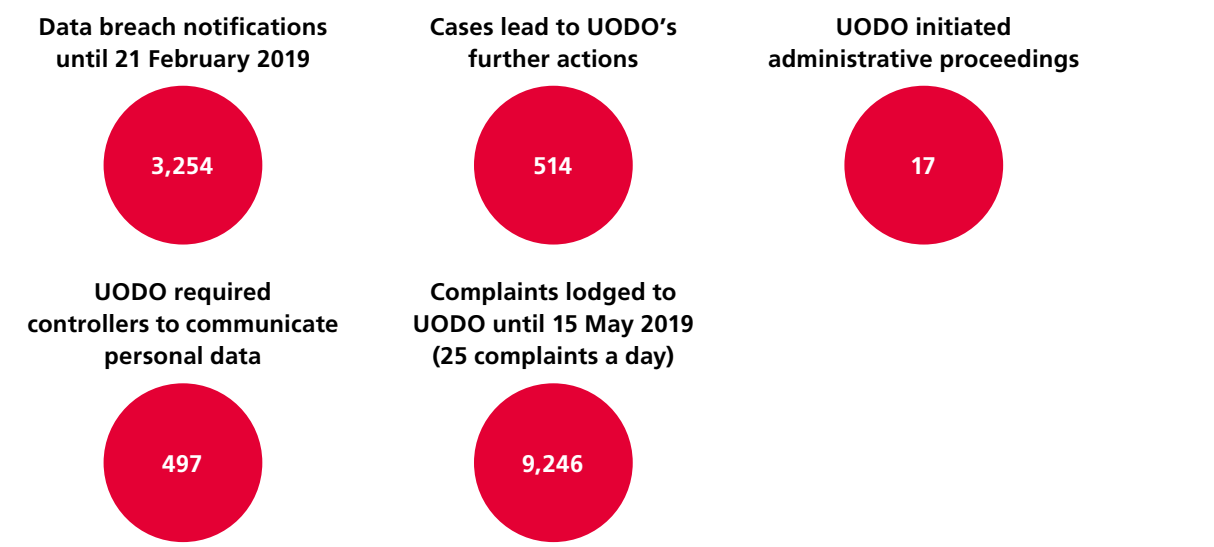
 **Marton Domokos**
Senior Counsel
T +36 1 483 4824
E marton.domokos@cms-cmno.com

 **Katalin Horvath**
Senior Associate
T +36 1 483 4897
E katalin.horvath@cms-cmno.com

Poland

President of the Personal Data Protection Office (“**UODO**”)

Facts & figures



On 16 May 2019, a new President of the Personal Data Protection Office commenced his 4-year term of office.

Watch out for

- Specific local rules on employee monitoring (CCTV and monitoring of e-mails, Internet use), required catalogue of personal data that may be requested from employees and candidates, legal basis for processing candidate and employee data.
- Consent requirements for e-mail and telephone marketing communications.
- Fulfilling information obligations towards individuals.
- Inspections – according to the annual inspection plan, the UODO’s 2019 inspections will include:
- Entities from the telemarketing sector, banking and insurance entities.
- Employers for CCTV and processing personal data in recruitment (regardless of the sector in which they operate).



The UODO published manuals and videos with practical guidelines for:

- Using CCTV systems.
- Processing personal data in the workplace.
- Maintaining a record of data processing activities.
- The transfer of personal data from Poland to the UK after Brexit.
- A risk-based approach.



Operations requiring mandatory data protection impact assessment (DPIA)

- Working time monitoring systems and monitoring of tools used by employees (e-mail, Internet).
- Use of employee or customer biometric data for access control systems.
- Offering services to individuals for processing information of purely personal or household activities (e.g. cloud services, e-mail, e-books, “life-logging” apps).

UODO is expected to announce a revised version of the DPIA in the near future.



Local legislative updates in the field of data protection

- Polish data protection act of 10 May 2018.
- Sectoral act aimed at ensuring application of the 21 February 2019 GDPR, which came into force on 4 May 2019 and changed over 160 laws regarding data protection.



Notable cases and takeaways

What happened?	Takeaways...
<p>Fine of EUR 220,000 for failing to meet information obligations.</p> <p>The company runs a commercial database composed of over 7.5 million records of personal data collected from public registers. The company met the information obligation for only those persons for whom it had e-mail addresses. For individuals whose addresses or phone numbers were not available, the company decided not to comply, due to the costs of mailing information notices and because it uploaded an information clause to its website.</p> <p>According to UODO, costs should not be a factor in assessing whether to comply.</p>	<p>Companies should verify whether they meet information obligations under the GDPR for all individuals whose data they process.</p>
<p>Fine of EUR 13,000 for failing to ensure confidentiality and security of personal data.</p> <p>The fine was imposed on a sporting association, which unintentionally published the personal data of 585 sport judges on its website, including names, home addresses and national identification numbers, exposing them to the risk of unauthorised use of their data.</p> <p>When considering a fine, UODO noted that the association did not take sufficient measures to remove the disclosed data from website subpages after the breach. Data was removed only during OUDO proceedings.</p>	<p>Companies should verify whether technical and organisational measures are appropriate to the risks related to processing and are sufficient to safeguard the confidentiality and security of personal data.</p>

<p>During a City Hall inspection, UODO detected a failure with GDPR compliance concerning:</p> <p>(i) information clauses provided to individuals (i.e. information about the recipients of personal data and data retention periods were insufficient);</p> <p>(ii) records of processing activities (i.e. datasets were recorded, not processing activities); and</p> <p>(iii) the agreements on entrusting personal data for processing (i.e. failure to meet requirements under Article 28 GDPR).</p> <p>No financial penalty was imposed, but the Mayor was ordered to bring its activities into compliance with the GDPR.</p>	<p>Companies should revise their information clauses, records of processing activities and data entrustment agreements to meet all GDPR requirements.</p>
<p>An insurance company identified a data breach but failed to provide affected individuals with information about (i) likely consequences of the breach and (ii) measures taken or proposed to address the breach.</p> <p>No financial penalty was imposed, however, UODO ordered the insurer to communicate the data breach to the affected individuals.</p>	<p>Companies should be prepared to send a clear communication if a breach to the individuals affected. They should ensure that the communication contains all information required under the GDPR.</p>

For further information, please contact:



Tomasz Koryzma
Partner
T +48 22 520 84 79
E tomasz.koryzma@cms-cmno.com



Damian Karwala
Senior Associate
T +48 22 520 83 38
E damian.karwala@cms-cmno.com



Paulina Komorowska
Associate
T +48 22 520 83 79
E paulina.komorowska@cms-cmno.com

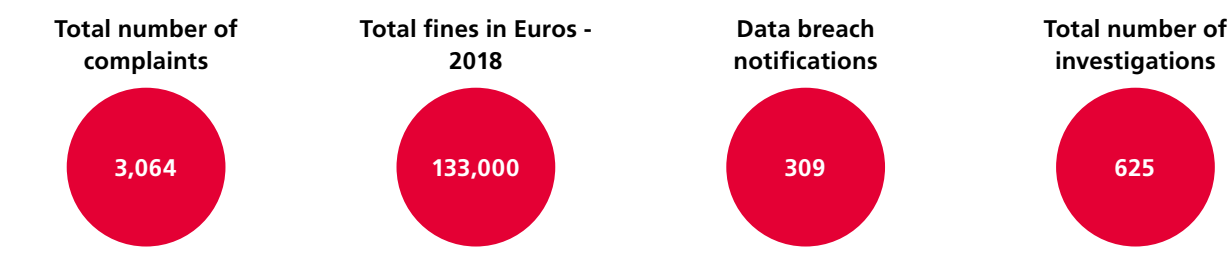


Romania

National Supervisory Authority for Personal Data Processing (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal or “ANSPDCP”)

Facts & figures

GDPR Statistics (time frame: 25 May 2018 – 31 December 2018) (as per media releases concerning an event organized by ANSPDCP on 28 January 2019 regarding the GDPR)



Watch out for

- Romanian legislation sets out stricter rules than the GDPR with regard to processing the so-called “national identification numbers” (such as personal identification number, the series and number of the identity document, the passport number, the driving licence number, the social health insurance number). When processing national identification numbers for a legitimate interest, the controller shall respect specific conditions.
- Strict conditions under which video surveillance of employees is permitted at work.
- Processing personal data for scientific or historical research purposes, statistic or archiving purposes are exempted from the GDPR rules.
- Political parties, NGOs or national minority’s organisations can process personal data without the express consent of the data subject.
- Less restrictive sanctioning system for public authorities (fines up to the maximum of approximately EUR 43,000).

Other specific guidance from the regulator

- Special procedures for receiving and solving complaints.
- Performing the investigations by ANSPDCP.
- Standard forms for personal data breach notification, and appointing the Data Protection Officer.

The regulator’s list on mandatory data protection impact assessments

- When automatic processing produces effects on the individual;
- Large-scale processing of sensitive data.
- Monitoring public areas (stadiums, markets, parks) on a large scale.
- Monitoring or systematic recording of behaviour of vulnerable persons (especially minors and employees) on a large scale.
- Using new technologies, especially where those limit the ability of data subjects to exercise their rights (e.g. facial recognition techniques to facilitate access to different locations) on a large scale.
- Processing data generated by sensor devices on a large scale.
- Wi-Fi and location tracking when processing is not requested by the data subject.

Complaints received under the GDPR concerned the following main areas:

- Video surveillance.
- Spam - receiving unsolicited commercial messages by voice call, e-mail, or SMS.
- Intentional leakage of personal data to the public (on the internet).
- Violation of certain rights of individuals expressly provided for in GDPR.
- Inappropriate/unacceptable use of cookies.
- Failure to comply with the conditions for consent in the online environment.
- Non-compliance with privacy by design / privacy by default.
- Concrete measures by operators regarding the security of the processing of personal data.

For further information, please contact:



Gabriel Sidere
Managing Partner
T +40 21 407 3813
E gabriel.sidere@cms-cmno.com

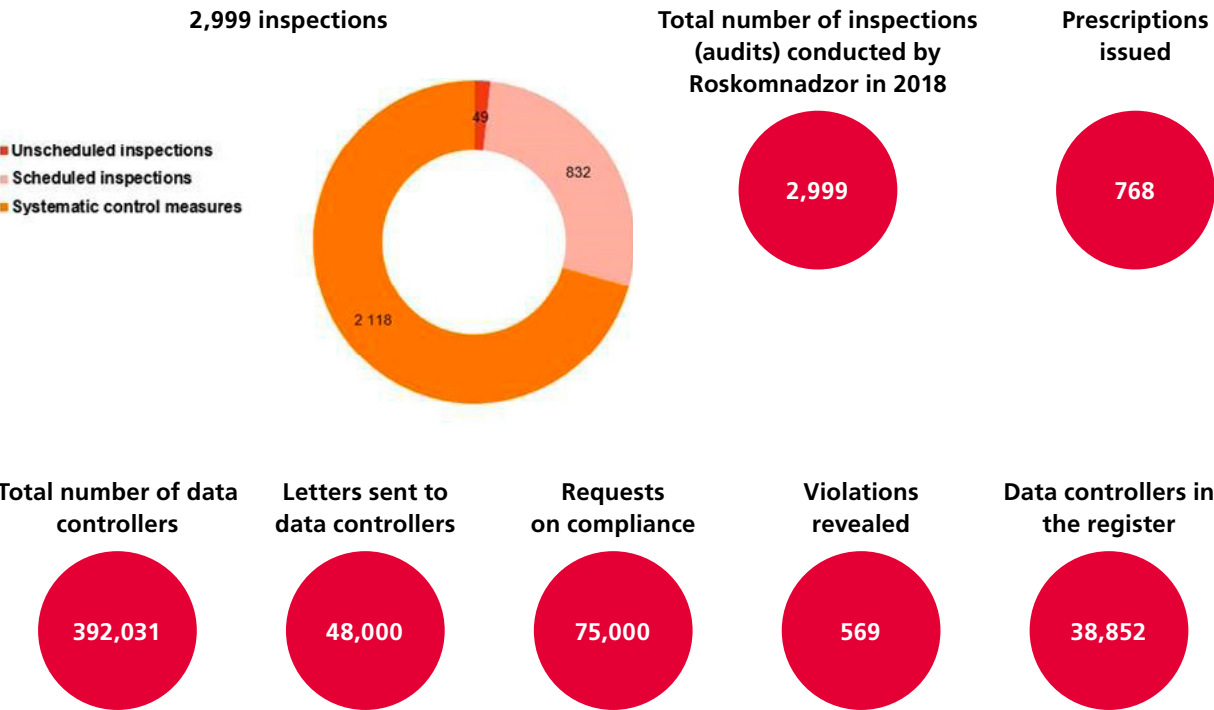


Valentina Parvu
Senior Associate
T +40 21 407 3825
E valentina.parvu@cms-cmno.com

Russia

Federal Service for Supervision of Communications, Information Technology and Mass Media (in Russian: Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций) or Roskomnadzor (in Russian: Роскомнадзор).

Facts & figures



GDPR

- If a Russian company or individual operates business in EU and processes personal data within the activity of that business.
- If the data subject, to whom a Russian company or individual processes personal data in order to provide goods and services, is in the EU during the data processing activity.
- If a Russian company or individual processes personal data in order to monitor consumer behaviour in EU.
- If any EU member state's law is applied to the given case.



Watch out for

- Accuracy of information provided to Roskomandzor.
- List of data protection measures.
- Lack of places to store personal data.
- Absence of a list of persons authorised to process personal data.
- Failure to notify Roskomnadzor regarding changes in data processing activities.
- Failure to comply with data retention requirements.
- Data processing in cases not prescribed by Russian law.
- Failure to comply with data minimisation principle.
- Improper forms of consent.



Other specific guidance from the regulator

- Availability of privacy policies on websites.
- Data localisation rules (initial collection and storage of Russian citizens personal data in Russia).
- Attention to cross-border transfers.
- Necessity to obtain consent for each separate processing purpose.



Notable cases and takeaways

What happened?	Takeaways...
Blocking of website due to the illegal publishing of personal data.	Companies shall ensure that personal data is published on the website based on the relevant consent of data subjects.

For further information, please contact:



Anton Bankovskiy
Partner
T +7 495 786 40 00
E anton.bankovskiy@cmslegal.ru



Vladislav Eltovskiy
Associate
T +7 495 786 4000 /4090
E vladislav.eltovskiy@cmslegal.ru

Slovakia

Office for Personal Data Protection of the Slovak Republic (Úrad na ochranu osobných údajov Slovenskej republiky)

Watch out for

- Specific local rules on background checks, photocopying of official documents, employee monitoring, processing of employee data, CCTV operations and entry systems, operating whistleblowing systems, processing of health data, processing of genetic data, anti-money laundering measures, and processing of national identification numbers.
- Opt-in” system for electronic direct marketing advertisements, unless direct marketing affects the goods and services possessed by the person who obtained electronic contact details in connection with the sale of goods or services.



Other specific guidance from the regulator

- Legal processing of personal data in clinical trials.
- Methodology of compliance of personal data processing in school environment.
- Methodological guidance on the legality of processing.
- Frequently asked questions about photos and audio-visual recordings.
- Opinion on the service of documents in administrative proceedings and the inspection of the administrative file.
- Position of legal entities and natural persons - entrepreneurs from the perspective of personal data protection.
- Methodological guidance on the obligations of an e-shop operator.
- Terms “fundamental rights and freedoms” vs. “rights and freedoms” and how to identify them.
- Administration of a fan page on a social network by a data controller.
- Guidance concerning notification of data protection officers and their contact details.
- Data protection methodology for towns and municipalities.



The regulator’s list on mandatory data protection impact assessments

- Processing biometric data of natural persons for the purposes of individual identification of the natural person in connection with at least one criterion stated in guidelines of the Article 29 Data Protection Working Party.
- Processing genetic data of natural persons in connection with at least one criterion stated in guidelines of the Article 29 Data Protection Working Party.
- Processing of location data in connection with at least one criterion stated in guidelines of the Article 29 Data Protection Working Party.
- Processing operations where personal data has not been obtained from individuals.
- Evaluation or scoring.
- Assessment of credibility.
- Assessment of creditworthiness.



- Profiling.
- Monitoring of employees on the basis of serious reasons pertaining to the special nature of employer’s activity.
- Processing of personal data for the purposes of scientific or historical research without the consent of the data subject in connection with at least one criterion stated in the guidelines of the Article 29 Data Protection Working Party.
- Processing operations using new or innovative technologies in connection with at least one criterion stated in the guidelines of the Article 29 Data Protection Working Party.
- Systematic CCTV monitoring of public areas.
- Monitoring of persons by private detectives or security services.

For further information, please contact:



Petra Corba Stark
Partner
T +421 2221 115 01
E petra.corbastark@cms-cmno.com



Martina Novysedlakova
Associate
T +421 2221 115 03
E martina.novysedlakova@cms-cmno.com

Slovenia

Slovenian Information Commissioner (“Informacijski pooblaščenec Republike Slovenije”)

In Slovenia, a local act further implementing GDPR has not been adopted yet (referred to as “ZVOP-2”). Due to a setback in the legislative process, the Information Commissioner cannot impose sanctions based on the GDPR, but only based on the Data Protection Act (ZVOP-1), which was in force prior to GDPR and will remain in force until adoption of ZVOP-2.

Watch out for

- Specific local rules on CCTV operations, biometric data, direct marketing, employee data.
- ZVOP-2 - once it is adopted.



Other specific guidance from the regulator

- Data processing guidelines.
- DPIA guidelines.
- Guidelines on the transfer of personal data to third countries and international organisations under the GDPR.
- Guidelines on creating privacy policies on websites.
- Guidelines on using cookies.
- Video surveillance guidelines.
- Information on recipients or categories of personal data recipients, etc.
- <https://upravljavec.si/> - a website designed to help small and medium-sized businesses.



The regulator’s list on mandatory data protection impact assessments
https://www.ip-rs.si/fileadmin/user_upload/Pdf/Ocene_ucinkov/SI_DPIA_list_35-4_35-6_Slovenia_revised_21dec2018_OBJAVA_ZA_WEB.pdf

For further information, please contact:



Amela Žrt
Attorney at law
T +386 1 620 5230
E amela.zrt@cms-rrh.com



Irena Šik Bukovnik
Attorney at law
T +386 1 620 5231
E irena.sikbukovnik@cms-rrh.com



Turkey

The regulator on personal data security: Personal Data Protection Authority (Kişisel Verileri Koruma Kurumu – “KVKK”).

Primary law

Law on Protection of Personal Data (“Law no.6698”) - enacted by using GDPR as a reference.

GDPR

- If a Turkish company or individual operates a business in the EU and processes personal data within the activity of that business.
- If the data subject, to whom a Turkish company or individual processes personal data in order to provide goods and services, is in the EU during the data processing activity.
- If a Turkish company or individual processes personal data in order to monitor consumer behaviour in the EU.
- If any EU member state’s law is applied to the given case.

KVKK resolutions are not publicly disclosed, unless it relates to common malpractice.

Board resolutions



- Unlawful transfer of health data.
- Ad e-mails or ad text messages without consent.
- Unlawful access to data.
- Inadequate physical and administrative measures.
- Unlawful sharing of contact info, and retention of personal data.
- Failure to provide data processing information, destroy personal data, respond a data subject access request, and notify a data breach to the authority.

Data breach notifications



- Unlawful access to e-mails.
- Unlawful access to photos via social media.
- Unlawful access to location data.
- Unlawful access to credibility scores by banks.
- Unlawful access to payment information of customers.
- Cyber-attacks.



Watch out for

- Specific local rules on explicit consent, employee monitoring, CCTV operations and entry systems, checklist of physical and technical measures to process sensitive data.
- Specific rules on transfer of personal data outside Turkey - either upon explicit consent of the individual or by obtaining a clearance/adequacy decision from KVKK.
- “Opt-in” system for electronic direct marketing advertisements.



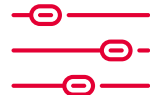
Other specific guidance from the regulator

- The content of an emergency response plan in case of a data breach occurs.
- The scope of personal data processing inventory including the details of data processing activities.
- Company policies on retention and destruction including the details of data processing activities.



Certain data controllers have to register with Turkish Data Controllers Registry's Online System (“VERBIS”)

- Who have more than 50 employees or whose total annual balance is more than TL 25,000,000 until 30 September 2019.
- Who have less than 50 employees and whose total annual balance is less than TL 25,000,000 but who process sensitive personal data as their main activity until 31 March 2020.
- Who are located abroad, without taking the number of employees or the annual balance amount into consideration until 30 September 2019.
- All public institutions and organisations processing any personal data until 30 June 2020.



Notable cases and takeaways

What happened?	Takeaways...
Warning on unlawful access to personal data by unauthorised staff members in the workplace.	Companies should revise their technical and administrative measures to prevent unauthorised access (e. g. placing separations or sound-proof windows between counters or pay-desks next to each other to prevent the presence of unauthorised people in such areas and to ensure that personal data disclosed in one service area cannot be heard, seen or learnt from the other).
Warning on the potential sanctions for non-compliance with the requirements for electronic direct marketing ads. An administrative fine in a range of between TRY 5,000 and TRY 1,000,000 may be imposed. The chief public prosecutor’s office notified of any non-compliance. Potential sanctions also include imprisonment.	Companies must ensure that they have their consumers’ preliminary consent to the receipt of advertisements.
Fine for a data breach (unlawful access). A pharmacist shared its customer’s sensitive personal (health) data with third parties.	Companies must take physical measures, such as keeping closed the customer files, locking the archive cabinet, destroying unnecessary documents containing personal data.

Warning for companies to take special measures for the protection of regularly processed sensitive personal data.	Companies should use encrypted hash, anti-virus software and similar secure methods if they retain sensitive personal data on computers, and also sign confidentiality agreements with their employees. A separate company policy is needed on data security requirements, specifically on sensitive data.
Warning to mobile applications and websites providing services such as accessing contact information by searching name or vice versa through collecting personal data from various applications, websites or social media accounts.	Processing contact information without consent is prohibited. Companies must delete any previously collected personal data if the individual did not give its consent to the processing.
Fine for failing to delete the name, address and phone number of a customer registered at the website of a clothing company.	Individuals have the right to ask the deletion of their personal data. Companies must send a response within 30 days and confirm the deletion of the relevant data in their filing system.
Fine for sharing the name, contact details and resume of a job applicant with affiliates, without the applicant's consent.	Affiliates within the same company group are different data controllers. The data transfer between such companies requires the explicit consent of the relevant individual.

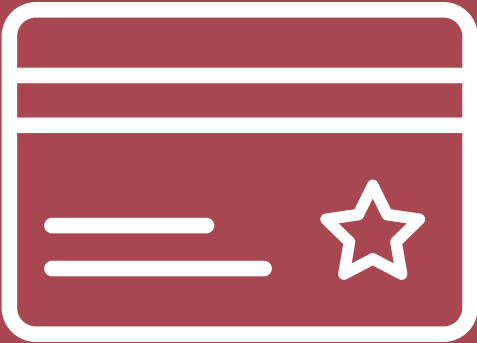
For further information, please contact:



Alican Babalioglu
Partner
T +90 212 401 42 60
E alican.babalioglu@cms-cmno.com



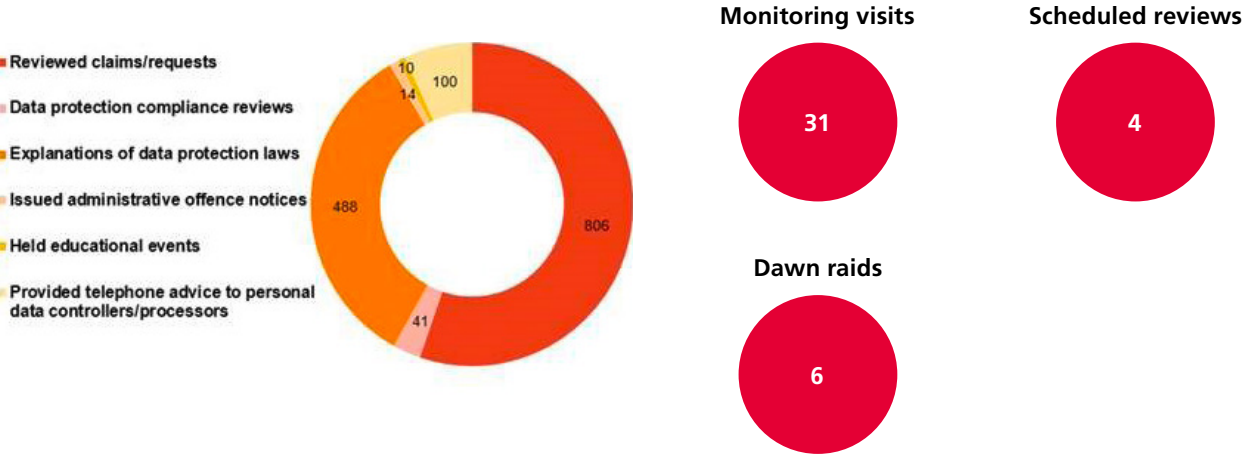
Inci Alaloglu-Cetin
Senior Associate
T +90 212 401 42 60
E inci.alaloglu-cetin@cms-cmno.com



Ukraine

Ukrainian Human Rights Ombudsman (Уповноважений Верховної Ради України з прав людини – “Ombudsman”). Official website: <http://www.ombudsman.gov.ua/ua/page/zpd/>

Main results of the Ombudsman's work in 2018



Certain Ukrainian companies may fall within the scope of the GDPR

- In certain cases, the GDPR is applicable inter alia to the processing of personal data by the organisations established outside of the European Economic Area.
- During the first year of the GDPR’s life, there were no clear-cut precedents of extra-jurisdictional enforceability of the GDPR. As a result, companies in Ukraine still do not have a clear understanding of how the GDPR may affect their business.
- Meanwhile, Ukraine is working on aligning its own legal framework to European standards. In particular, under the EU-Ukraine Association Agreement, Ukraine has made a commitment to bring national personal data protection legislation in line with the GDPR.
- In October 2017, the Ukrainian government approved the EU-Ukraine Association Agreement Implementation Plan. One of the steps of this plan is to develop and adopt a new draft law on processing of personal data, which should be closely based on the GDPR.
- On 25 April 2018, the official Ukrainian translation of the GDPR was approved by the government (<https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf>).
- In October 2018, the Ombudsman, who is responsible for the development of a new draft law, arranged the first public discussions with the business community regarding the draft law. As of May 2019, the draft was not fully prepared yet, and Ukrainian business is waiting for updates.
- While the new legislation is underway, the main act governing the processing of personal data in Ukraine is the Law of Ukraine on Personal Data Protection (PDP Law) dated 1 June 2010. Below is the brief overview of the regulator’s work in 2018.

Main types of violations identified by the regulator in 2018

- Inappropriate notification to the regulator on the processing of high-risk data.
- Not obtaining written statements of non-disclosure of personal data from the employees who have access to personal data.
- Failure to notify individuals about the composition and content of collected personal data.
- Not determining the person responsible for the protection of processed personal data.

The regulator’s list of recommendations for business

- To amend/develop internal policies in accordance with the personal data law requirements (regulating the procedure of processing of personal data, access to such data, recording of data processing operations, etc.).
- To stop requesting personal data consent in cases, where personal data is processed on the grounds specified by the law.
- To set up reasonable time limits for the storage of personal data and to ensure that data is not processed out of these limits.
- To obtain written statements of non-disclosure of personal data from employees who have access to personal data during the performance of their job duties.
- To develop and adopt the internal policy/plan for cases of unauthorised access to personal data, cyber incidents, or other emergencies.

Notable cases

Name of the company/agency	What happened?
JSC Ukrainian Railways (a state-owned enterprise of rail transport in Ukraine that controls vast majority of the railroad transportation in the country)	The Ombudsman has audited and given recommendations to Ukrainian Railways for compliance with data protection law requirements in connection with the planned implementation of a video surveillance system in passenger cars.
Nova Poshta LLC (the largest national logistics company, particularly in post and delivery services)	Following media coverage of data leakage in the online delivery tracking system of Nova Poshta, the Ombudsman conducted a dawn raid of the company. As a result of the audit, the Ombudsman has not identified the violations committed by the company. Nova Poshta declared that it has introduced additional technical security measures in their online systems.
Centres of Administrative Services (government agencies for the provision of various administrative services)	The Ombudsman has carried out a data protection compliance review of administrative service centres in connection to inappropriate collection of personal data consents from Ukrainian nationals in the process of applying for passports. The regulator issued recommendations to the agencies.

For further information, please contact:



Olga Belyakova
Partner
T +380 44 391 7727
E olga.belyakova@cms-cmno.com



Mykola Heletiy
Associate
T +380 44 391 7732
E mykola.heletiy@cms-cmno.com

Information according to the Ombudsman’s 2018 Annual Report (in Ukrainian only).
<https://notorture.org.ua/wp-content/uploads/2019/04/Report-2019.pdf>



Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.
cms-lawnow.com

.....
CMS Cameron McKenna Nabarro Olswang LLP
Cannon Place
78 Cannon Street
London EC4N 6AF

T +44 (0)20 7367 3000
F +44 (0)20 7367 2000

The information held in this publication is for general purposes and guidance only and does not purport to constitute legal or professional advice.

CMS Cameron McKenna Nabarro Olswang LLP is a limited liability partnership registered in England and Wales with registration number OC310335. It is a body corporate which uses the word "partner" to refer to a member, or an employee or consultant with equivalent standing and qualifications. It is authorised and regulated by the Solicitors Regulation Authority of England and Wales with SRA number 423370 and by the Law Society of Scotland with registered number 47313. It is able to provide international legal services to clients utilising, where appropriate, the services of its associated international offices. The associated international offices of CMS Cameron McKenna Nabarro Olswang LLP are separate and distinct from it. A list of members and their professional qualifications is open to inspection at the registered office, Cannon Place, 78 Cannon Street, London EC4N 6AF. Members are either solicitors or registered foreign lawyers. VAT registration number: 974 899 925. Further information about the firm can be found at cms.law

© CMS Cameron McKenna Nabarro Olswang LLP

CMS Cameron McKenna Nabarro Olswang LLP is a member of CMS Legal Services EEIG (CMS EEIG), a European Economic Interest Grouping that coordinates an organisation of independent law firms. CMS EEIG provides no client services. Such services are solely provided by CMS EEIG's member firms in their respective jurisdictions. CMS EEIG and each of its member firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS EEIG and each member firm are liable only for their own acts or omissions and not those of each other. The brand name "CMS" and the term "firm" are used to refer to some or all of the member firms or their offices. Further information can be found at cms.law