Your World First

C/M/S/

Law.Tax

CEE Consumer Products Update

December 2016

Introduction

As the Internet of Things continues to emerge and to spread into every area of daily life, the regulation of legal aspects connected to these new technologies becomes more and more pressing. The development of smart products and devices is occurring at such an astonishing pace that jurisprudence and legislation can hardly keep up.

In April 2016 the European Commission issued Regulation (EU) 2016/679 (General Data Protection Regulation) that governs the protection of natural persons with regard to the processing of personal data and on the free movement of such data. As the regulation will enter into force after a two-year transition period that ends in May 2018, a lot of questions regarding these issues remain and will tend to increase until the official application date.

One of the most immediate problems concerns devices that collect and store personal data that is frequently transferred either automatically, for instance via Internet, or during maintenance of the devices to manufacturers or dealers respectively. This no longer affects just the IT branch, as a wide range of goods – including goods from the automotive industry, white goods and household appliances, as well as 'smart home' devices, collect and process data nowadays. Cars, for example, record valuable data on driving behavior, wear and tear of the car as well as fuel consumption. Does this constitute personal data or is it only related to the product itself? Given that the owner of a car can be identified through serial numbers, this is an open question. In any case, this information could be valuable not only to manufacturers but also to law enforcement agencies or insurers. The issue also applies to other products, as even washing machines or refrigerators collect data on their use. In a smart home, these devices are connected to and thus controllable by smartphones, which raises another significant problem: how do you control and protect yourself against the misuse of your data if – as researchers have discovered – it is possible for hackers to gain access to your Wi-Fi network through a simple thing like a Wi-Fi enabled light bulb?

From the legal perspective, it can be asked if, for example the frequency of use or the location of a device qualifies as personal data. If so, does the use and storage depend on domestic law? And if the local law that governs the manufacturer is applicable – what happens if the jurisdiction of the consumer contradicts the provisions in the governing law under which the manufacturer operates? On a European level, Regulation 2016/679 could provide consistency and uniformity, although Art. 23 contains a flexibility clause that allows for restrictions on a national level in substantiated exceptional cases.

Nevertheless, trade of consumer products occurs more and more on a global level, and not all countries apply the same high standards regarding data protection.

In this bulletin we would like to answer four major questions as regards some important economies in the CEE-Region like Bulgaria, the Czech Republic, Hungary, Poland and Romania.

The questions are as follows:

1. When does data qualify as personal data?
2. Which law is applicable for the storage and processing of data?
3. Under what conditions are the storage and processing of data/personal data allowed according to local law?
4. Are any changes expected in your jurisdiction in the light of Regulation 2016/679?

Martin Wodraschke
Partner, Head of CEE Automotive
T +36 1 483 4828
E martin.wodraschke@cms-cmck.com

Executive summary

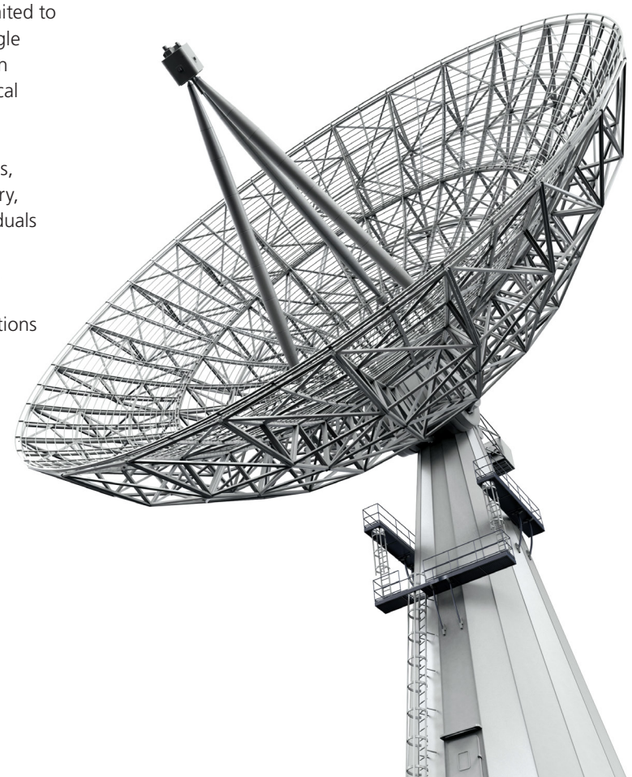
The new national Data Protection laws that are being considered treat 'personal data' as information on individuals (not legal entities). Furthermore, what exactly constitutes personal data must be determined on a case-by-case basis and is not named in exhaustive lists.

Information that is related to natural persons and references drawn from such information are deemed to be personal data as long as the identification of an individual is possible. Moreover, all the jurisdictions specifically address the topic of 'sensitive' personal data, such as the ethnicity, attitudes, convictions and beliefs of an individual.

Each of the five jurisdictions' data protection law is based on Directive 95/46/EC and is usually supplemented by secondary legislation in specific areas. The respective acts set out a general framework containing such aspects as the definition of personal data, rules on data processing and data transfer, consent rules, rights and remedies etc. Typically, a specific national authority is established for the purpose of enforcing and interpreting the Data Protection Acts. Generally, the applicability of national laws is limited to the respective territory of the state, whereas single provisions also address data processors in foreign countries provided that they make use of technical means located in the respective territory.

For the purpose of processing data on individuals, each of the jurisdictions requires a prior, voluntary, express and informed consent from those individuals with specific exceptions ranging from certain statutory grounds to a 'legitimate interest' basis. The concrete demands that such consent must meet as well as the spectrum of statutory exceptions might differ slightly between jurisdictions.

While – with regard to the General Data Protection Regulation (GDPR, i.e. Regulation 2016/679) that was enacted in April 2016 and that enters into force in May 2018 repealing Directive 95/46/EC – no legislative changes in the Czech Republic, Hungary and Romania have occurred yet, as the authorities are presumably waiting for the Regulation to enter into force and to subsequently repeal or amend provisions that will then be governed by the Regulation, the Bulgarian and the Polish authorities seem to be engaged in legislative works already. The Ministry of Administration and Digitalization in Poland is addressing topics that were left to the discretion of the Member States, whereas the Bulgarian Personal Data Protection Commission is currently working on a draft of a new Data Protection Act that will be in line with Regulation 2016/679.



Bulgaria

When does data qualify as personal data?

Art. 2, paragraph 1 of the Bulgarian Data Protection Act (the 'DPA') 'personal data' refers to any information related to an individual who is identified or identifiable, directly or indirectly, by reference to an identification number or to one or more specific features.

The DPA does not provide an exhaustive list of data which is considered 'personal data', so this must be assessed on a case-by-case basis. The Bulgarian Personal Data Protection Commission (the 'PDPC'), in its established case law deems the following data as personal data: names, personal identification number, address, telephone number, place of birth, passport data of the person (physical identity); marital status and kinship (family identity); professional background (work), etc. Furthermore, Article 5, paragraph 1 of the DPA, sets forth a special category of data (so-called 'sensitive personal data') which includes personal data revealing: (1) racial or ethnic origin; (2) political, religious or philosophical convictions, membership in political parties or organizations, associations having religious, philosophical, political or trade-union goals, and (3) health, sex life or human genome. The processing of such sensitive data is prohibited, except for in a number of statutory exceptions.

Which law is applicable to the storage and processing of data?

The Bulgarian DPA is based on Directive 95/46/EC and sets the general framework for data protection in Bulgaria. It defines personal data and data processing, regulates consent rules, data transfer, the obligations of data controllers and data processors and the rights and remedies of the relevant data subjects. The DPA applies to the processing of personal data where the data controller: (i) is established in the territory of the Republic of Bulgaria and processes personal data in regard to their activity; (ii) is not established in the territory of the Republic of Bulgaria but must apply the DPA by virtue of international public law; or (iii) is not established in the territory of the EU or the European Economic Area (EEA), but, for the purposes of such processing, makes use of means located in the territory of the Republic of Bulgaria (unless such means are being used exclusively for transit purposes).

The PDPC is the statutory authority vested with the right to ensure the protection of the rights of individuals when their personal data is being processed, as well as the right to monitor for compliance with the DPA.

Under which conditions are the storage and processing of data/personal data allowed according to your local law?

Similar to other EU jurisdictions, under Bulgarian law personal data may be processed if the data subject's consent was granted or if one of the statutory grounds (as set out under Art. 4 of the DPA) is met.

Consent under the DPA shall mean 'any freely given, specific and informed statement of volition by which the data subject signifies unambiguously his or her consent to such data being processed.' The consent of the data subject must be explicit, i.e. it must contain the purpose of the data processing. No particular form is required by the DPA. Written form is not an absolute requirement, but in practice it is impossible to evidence the express, specific and informed consent without a written document. The data controller must always be in the position to prove that consent was provided in compliance with the law, so proper archiving is advisable.

Other statutory grounds for processing personal data would include:

- for compliance with a statutory obligation applicable to the data controller;
- for the fulfilment of obligations under an agreement to which the data subject is party, as well as for any activities initiated by the same individual prior to the conclusion of the agreement;
- or the protection of the life and health of the data subject;
- for the performance of a task carried out in the public interest;
- for the exercise of an official authority vested by law in the controller or in a third party to whom the data is disclosed;
- for the realization of the legitimate interests of the data controller or a third party, except where such interests are overridden by the interests of the data subject.

Are any changes expected in your jurisdiction in the light of regulation 2016/679?

Yes. The PDPC plans for the preparation of a new DPA that would be compliant with the new Regulation 2016/679 (most likely this will happen closer to the start date of the application of the new Regulation: 25 May 2018).

Assen Georgiev
Partner
T +359 2 921 9936
E assen.georgiev@cms-cmck.com

Czech Republic

When does data qualify as personal data?

Act 101/200 Coll. on the Protection of Personal Data ('Data Protection Act') only applies to information about individuals (natural person / data subject) as opposed to legal entities. Similarly to Directive 95/46/EC, the Data Protection Act does not provide an exhaustive list of data which is considered 'personal data', so this must be assessed on a case-by-case basis. Personal data means any information relating to an identified or identifiable data subject. A data subject will be considered identified or identifiable if it is possible to identify the data subject directly or indirectly in particular on the basis of a number, code or one or more factors specific to his/her physical, physiological, psychical, economic, cultural or social identity. In line with Article 8 of Directive 95/46/EC, the Data Protection Act sets forth a special category regarding 'sensitive data' meaning: personal data revealing nationality, racial or ethnic origin, political attitudes, trade-union membership, religious and philosophical beliefs, conviction of a criminal act, state of health and sexual life of the data subject and genetic data of the data subject; sensitive data also means biometric data permitting the direct identification or authentication of the data subject.

Which law is applicable to the storage and processing of data?

Storage of personal data is regulated by the Data Protection Act and various other acts based on the data subject (e.g. Labour Code or Act on Accounting etc.).

The Data Protection Act is based on Directive 95/46/EC and sets out the general framework for data protection. In particular, it defines personal data and data processing, regulates consent rules, data transfer, the obligations of data controllers and processors and the rights and remedies of the relevant persons. The Data Protection Act can be found under the link. The Data Protection Act applies to all data processing operations performed in the Czech Republic that involve personal data. The Data Protection Act also applies if a third-country controller engages a data processor in the Czech Republic, unless it is only a personal data transfer over the territory of the European Union. If the controller carries out processing through its organization units established on the territory of the Czech Republic, he must ensure that those organization units will process personal data in accordance with national law.

Under which conditions are the storage and processing of data/personal data allowed according to your local law?

Personal data may be processed with the consent of the individual or if the processing is allowed by law. When sensitive data is processed explicit consent must be given. When giving consent the data subject must be provided with information about the purpose of processing, what personal data is to be processed, who the data controller is, and the period of time the consent is being given for. The controller must be able to prove the consent of the data subject to the personal data processing for the whole period of the processing. The controller is obliged to specify the purpose for which personal data is to be processed and specify the means and manner of personal data processing. The controller is also obliged to collect personal data corresponding exclusively to the specified purpose and to the extent necessary to accomplish the specified purpose as well as store personal data only for a period necessary for the purpose of their processing. After the expiry of this period, personal data may be retained only for the purposes of the state statistical service, and for scientific and archival needs. When using personal data for these purposes, it is necessary to respect the right to protection of the private and personal lives of the data subject from unauthorized interference and to make the personal data anonymous as soon as possible. Other obligations of the controller include processing personal data only in accordance with the purpose for which the data were collected and collect personal data only in an open manner. Collecting data under the pretext of some other purpose or activity is prohibited. The controller is also obliged to ensure that the personal data that was obtained for different purposes is not grouped. The obligations specified similarly apply to processors.

Are any changes expected in your jurisdiction in the light of Regulation 2016/679?

The Data Protection Act has not been amended and does not yet reflect any changes introduced by Regulation 2016/679. It is possible that Parliament will wait until the Regulation becomes directly applicable in May 2018 and will repeal or amend the provisions of the Data Protection Act which are governed by the Regulation.

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

Hungary

When does data qualify as personal data?

Act CXII of 2011 on the Right of Self-Determination in Respect of Information and the Freedom of Information ('Data Protection Act') only applies to information about individuals as opposed to legal entities. Like Directive 95/46/EC, the Data Protection Act does not provide an exhaustive list of data which is considered 'personal data', so this must be assessed on a case-by-case basis. Personal data means any information relating a natural person and any reference drawn from such information. Such information will be treated as personal data as long as the data controller / data processor has the necessary technology to identify the relevant person. In line with Article 8 of Directive 95/46/EC, the Data Protection Act sets forth a special category of data ('sensitive personal data') which means: (1) personal data revealing racial, national or ethnic origin, political opinions and any affiliation with political parties, religious or philosophical beliefs, trade-union membership, and (ii) personal data concerning health, addictions, sex life, or criminal record.

Which law is applicable to the storage and processing of data?

The Data Protection Act is based on Directive 95/46/EC and sets the general framework for data protection. To be precise, it defines personal data and data processing, regulates consent rules, data transfer, the obligations of data processors and the rights and remedies of the relevant persons. The Data Protection Act can be found at the following link: http://www.naih. hu/act-cxii-of-2011---privacy-act--.html. The Data Protection Act applies to all data processing operations performed in Hungary that involve personal data. The Data Protection Act also applies if a third-country controller engages a data processor in Hungary or if it is using equipment in Hungary, unless such equipment is used solely for the purpose of transit through the EU. The Hungarian Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság – 'NAIH') tends to interpret the scope of the Data Protection Act extensively, based on the 'Weltimmo case' where a company established in Slovakia was fined because it operated a website containing advertisements of properties located in Hungary and collected personal data from Hungarian buyers and sellers. In such cases, the Court of Justice of the European Union (CJEU) has ruled that the data protection legislation of a Member State may apply to a data controller registered in another Member State if, through stable arrangements in the territory of that Member State, the data controller exercises a real and effective activity; however minimal, in the context of processing personal data.

Under which conditions are the storage and processing of data/personal data allowed according to your local law?

Personal data may be processed with the prior, voluntary, express and informed consent of the individual or if the processing is allowed by law. In practice, consent can be given verbally, in writing, electronically or by implication. Electronic consent may be acceptable through, e.g., a click by the relevant person on an 'acceptance button' or 'consent box'. Before ticking, the relevant person should also be given the opportunity to read the relevant privacy policy, which gives information on the data processing. Written consent is required only for processing sensitive personal data (unless the data processing is required by law). If the consent is provided electronically and the relevant person is identifiable unambiguously, NAIH considers it as being in writing. The data controller must always be in the position to prove that consent has been provided properly and lawfully, so proper archiving is advisable. NAIH also pointed out that the consent is not free and express if the 'yes' checkbox is ticked in advance by default and does not require any action from the user besides proceeding with the registration.

Personal data can also be processed if obtaining the consent proves impossible or involves a disproportionate cost and if the processing is necessary for:

— compliance with a legal obligation applicable to the data controller, or

— the purpose of legitimate interests of the data controller or third parties and such necessity is proportionate to the restriction of privacy.

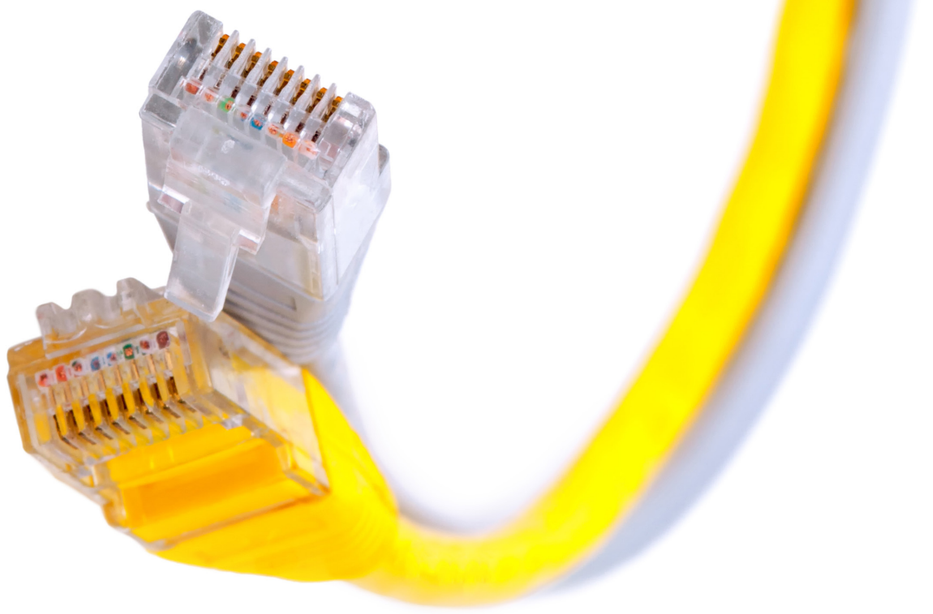
In the aforementioned cases data may also be processed if the relevant person withdraws his/her consent (which can be done at any time under the law). This 'legitimate interest' exception may be applied, for example, in cases where data is necessary for a technical operation – e.g. transmitting the personal data of employees to an IT database due to outsourcing – but would require unreasonable administration and effort to collect the consent individually or if only one person does not consent to the processing, if this can unreasonably delay or prevent the achievement of the desired goal. According to NAIH, the term 'legitimate interest' covers 'lawful and fair business interests'.

To rely on the 'legitimate interest basis', controllers must perform a so-called 'balance of interests' test, where they identify the legal interest of the data controller, the data subject and the underlying fundamental right, and whether the personal data may be processed as the result of the balancing. Data subjects should be informed on the result of the test (why the legitimate interest is more important than the underlying privacy rights and interest of the data subject). Data subjects should be informed of the data protection measures undertaken with a view to the lack of consent, and the possibility to object to the processing.

Are any changes expected in your jurisdiction in the light of Regulation 2016/679?

The Data Protection Act has not yet been amended to reflect any changes introduced by Regulation 2016/679. It is likely that Parliament will wait for the date when the Regulation becomes directly applicable – 25 May 2018 – and will repeal those provisions of the Data Protection Act which are governed by the Regulation around that date. It is worth noting, however, that NAIH already applies in its practice certain concepts which were introduced only by the Regulation. For example, NAIH provides that in the case of voice recordings data access rights include receiving a copy of the voice recording for free. This specific right is not contained in the Data Protection Act but NAIH considers the Regulation as a guideline, which will require the controller to provide a copy of the personal data undergoing processing.

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



Poland

When does data qualify as personal data?

The Act of 29 August 1997 on Personal Data Protection ('Data Protection Act') does not provide an exhaustive list of the data which is deemed to be 'personal data'. Personal data is defined as any information that relates to an identified or identifiable individual (the data subject). However, while the first part of this definition is quite straightforward, the part which refers to an identifiable person is more complicated, in particular in the light of new kinds of data. Hence, under Polish law for example a Vehicle Information Number ('VIN') is not information based on which the data subject is or can be identified; therefore, it does not constitute personal data as such. However, it would be considered as personal data if it is combined with other data that can lead to a particular data subject.

Moreover, the Data Protection Act sets a special category of data – 'sensitive personal data'. Sensitive personal data is (a) data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, political party or trade-union membership as well as (b) personal data concerning health, genetic code, addictions and sexual orientation, or criminal record, and finally (c) personal data relating to criminal convictions, decisions on penalties, fines and other decisions issued in court or administrative proceedings.

One of the most controversial kinds of data in Poland is biometric data, very often processed for the purpose of controlling working hours. Processing such employee data has been the subject of many court decisions, being seen as not accurate for the purposes for which it is processed, but was not regulated until Regulation 2016/679 came into force.

Which law is applicable to the storage and processing of data?

The Polish Data Protection Act applies to public entities, such as national authorities and local government authorities, as well as to private entities, in particular:

— non-public bodies that carry out public tasks, and

— individuals, legal entities and organizational units that are not legal entities.

The Data Protection Act is applicable to individuals, legal entities and organizational units, provided that they are involved in processing personal data as part of their business or professional activity and if the registered office or place of residence is located in the territory of Poland. If data is processed in a third country, the Polish data protection regime would still apply if personal data using technical measures located in the territory of Poland were to be processed.

Under which conditions are the storage and processing of data/personal data allowed according to your local law?

Personal data processing (e.g. storage) is allowed under Polish law when one of the statutory, legal bases set forth in the Data Protection Act applies. In most cases, the data subject's prior, voluntary, express and informed consent is required before personal data can be processed. Consent of the data subject is the most common legal basis for processing data. No specific form of the data subject's consent is required. Electronic consent may be acceptable through an 'acceptance button' or 'consent box'. However, processing sensitive data as well as the transfer of data outside the European Economic Area requires written consent. For evidential purposes, written consent is advisable in every case of processing data on this basis, since the data controller should always be in a position to prove that the consent has been provided properly and lawfully.

Personal data can also be processed if the processing is allowed according to the Polish data protection regime, when it is necessary to enforce a right or comply with legal obligations (such as in the case of legal representation under granted power of attorney). Processing can also be based on other grounds as for example when it is necessary in order to perform a contract. One of the most popular bases concerns the so-called 'legitimate interest' of the data controller. The latter can be problematic, however, since in order to use such a basis the controller must be able to prove that processing does not violate the rights and freedoms of data subjects. According to the Data Protection Act, legitimate interest is considered to be, in particular, direct marketing of the controller's products or services or pursuit of claims associated with economic activities.

Are any changes expected in your jurisdiction in the light of Regulation 2016/679?

We are aware of legislative works that currently take place in the Ministry of Digitalization. The works are aimed at implementing the GDPR in the scope that was left to the Member States to regulate, e.g. concerning the conditions for processing personal data or the mandatory data protection officer. We may expect that the works will be finished within the next year.

Marcin Lewoszewski
Senior Associate / Attorney at Law
T +48 22 520 5525
E marcin.lewoszewski@cms-cmck.com

Romania

When does data qualify as personal data?

Romanian Data Protection Law defines 'personal data' consistently with the EU Data Protection Directive (Directive 95/46/EC), that is 'any information related to an individual/natural person who is identified or identifiable, whether directly or indirectly, in particular by reference to an identification number or one or more factors which are specific to his/her physical, physiological, psychological, economic, cultural or social identity'. This definition provides an umbrella potentially encompassing a very wide range of data. While with respect to some data (e.g. name, personal numeric code, social security number etc.) this qualification as 'personal data' will be immediately obvious, others may need to be assessed on a case-by-case basis to see if they meet the conditions of the definition.

The Romanian Data Protection Law also makes specific reference to special or sensitive categories of data, which are subject to stricter requirements with respect to processing, disclosure and transfer. Such special/sensitive data include: data relating to race or ethnic origin; political, religious, philosophical or similar beliefs; trade union membership; health data; data relating to sexual life; personal identifiers; criminal convictions or safety measures.

Which law is applicable to the storage and processing of data?

The framework legislation regulating the processing of personal data in Romania is the Romanian Data Protection Law. Further specific provisions relating to the processing of personal data in the electronic communications sector are found in the Romanian Electronic Communications Privacy Law.

The Romanian Data Protection Law sets the general legal framework regulating the processing of personal data, by defining: (i) who is within its scope (i.e. data controllers established in Romania, or foreign data controllers if they process personal data through any means located in Romania, unless such means are used for transit purposes exclusively); (ii) the main concepts (i.e. data controller, personal data, data processor, transfer, disclosure, recipient, third party etc.); (iii) principles of data processing; (iv) rules applicable to consent; (v) conditions for the processing of sensitive/special personal data; (vi) rules for appointing data processors; (vii) rules on transfers of personal data abroad; and (viii) breaches and applicable sanctions.

The Romanian Data Protection Law is supplemented by an array of secondary legislation issued by the Romanian Data Protection Authority – such secondary legislation regulates, inter alia, when processing of personal data is exempt from notification; model clauses that may be used for controller to controller, or controller to processor data transfers; technical and organizational measures that must be implemented to ensure data confidentiality/security; authorization of data transfers abroad to third countries (i.e. non EU/EEA countries, which are not recognized as ensuring an adequate level of protection of personal data); conditions for processing specific data (e.g. sensitive data) or through specific means (e.g. video surveillance).

Under which conditions are the storage and processing of data/personal data allowed according to your local law?

Consistent with the EU Data Protection Directive, Romanian data protection legislation provides that personal data must be (a) processed in good faith and in accordance with the law; (b) collected for a determined, explicit and legitimate purpose and not further processed outside of that scope (unless for statistical, historical or scientific research purposes); (c) adequate and relevant for the purposes for which they were collected [data minimization]; (d) exact/accurate and, where needed, updated; (e) stored in a form that allows for the identification of the data subjects strictly for the duration needed to satisfy the purpose for which the data was collected.

As a rule, processing of personal data should be based on the explicit, unambiguous, informed and freely given consent of the data subject. The law does not require a specific form of consent (although the Romanian Data Protection Authority does provide template forms for guidance). Consent must however be express and unambiguous and relate to that specific processing (and processing purpose) for which it is given.

Romanian data protection law provides for derogations/exceptions from the informed consent rule, e.g. (i) when processing is necessary for the purposes of performing a contract to which the data subject is a party, or for the purposes of taking measures – at the request of the data subject – for entering into a contract; (ii) when processing is necessary to satisfy a legal obligation of the data controller; (iii) when processing is necessary to protect the life, bodily integrity or health of the data subject or another individual at risk; (iv) when processing is necessary for public interest measures; (v) when processing is necessary for the purposes of satisfying a legitimate interest of the data controller or the third party to whom the data is disclosed, provided however that such interest is not overridden by the fundamental rights and freedoms of the data subjects; (vii) when processing refers to data that is obtained from publicly accessible documents/sources; or (viii) when processing is done exclusively for statistical purposes, or for historic or scientific research.

Depending on the category of data processed, and especially with respect to special/sensitive data, not all of the exceptions above (or any) will apply. Any data controller needs to clearly assess the legal basis which legitimizes its processing of personal data (where informed consent does not apply). When relying on 'legitimate interests' as the legal basis for processing, data controllers should perform a so-called 'balance of interests' test between the interests of the data controllers and those fundamental rights and freedoms of the data subjects that may be adversely impacted by the processing.

In all cases, all data controllers must ensure that they implement adequate technical and organizational procedures to ensure the confidentiality and security of the personal data processed, in line with the minimum security requirements set forth by the Romanian Data Protection Authority (these regulate, inter alia, access to personal data; making back-up/safety copies; keeping logs to record any access to, and operation on, the personal data; training of personnel in data protection matters etc.).

Are any changes expected in your jurisdiction in the light of Regulation 2016/679?

It is expected that a large portion of the existing Romanian data protection legislation will be repealed entirely and replaced with the General Data Protection Regulation (the 'GDPR') as of 25 May 2018. Nevertheless, despite being a Regulation, the GDPR makes provision for Member States legislating in many areas.

Member States are able to implement derogations from the GDPR, where they are required for the purposes of national security, prevention and detection of crime, other important public interests, in particular economic or financial interests (e.g. budgetary and taxation matters) etc. Where such derogations are made at the national level, they must nonetheless 'respect the essence of … fundamental rights and freedoms and be … necessary and proportionate … in a democratic society'.

Other special topics where Member State law is foreseen include processing of employee data; processing in connection with freedom of expression and professional secrecy (where restrictions of supervisory authority audit rights are foreseen); conditions for processing national identification numbers: archiving in the public interest etc. So far, the Romanian Data Protection Authority has not publicly expressed any opinion as to its plans for implementation of the GDPR or a timeline for the same.

One of the more relevant changes to the GDPR which is expected to produce a substantial impact is the extension of the scope of cover – whereas previously non-EU established organizations were not subject to national data protection rules (unless processing data through means e.g. a server located in Romania), they will now be caught under the rules where they process personal data about EU data subjects in connection with the offering of goods or services, or monitoring their behavior within the EU. It will be interesting to see how such organizations, which were not previously within the scope, will be forced to comply with the GDPR and how sanctions for default will be imposed against them.

Cristina Popescu
Senior Associate
E cristina.popescu@cms-cmck.com

Consumer Products Sector Focus Group in CEE

Our Consumer Products Sector Focus Group provides advice on everything from the financing and acquisition of companies through to regulatory aspects, competition and dawn raids, media litigation procedures, brand protection strategies, outsourcing and distribution agreements, real estate transactions, packaging and labelling as well us product recalls within the consumer products sector.

Our clients include leading industry players in everything from food & drink, health & beauty, cosmetics, clothing, sports, retailers, automotive, household equipment and electronics. We work with everyone from banks and investors to suppliers and regulators, providing specialist advice for all audiences. Our lawyers work together, with cross-border teams assembled when necessary, to ensure seamless international legal support.

If you are interested in our services, please contact us.

Bulgaria

Assen Georgiev
Partner
T +359 2 921 9936
E assen.georgiev@cms-cmck.com

Czech Republic & Slovakia

Frances Gerrard
Senior Associate
T +420 296 798 834
E frances.gerrard@cms-cmck.com

Hungary

Aniko Kircsi
Partner
T +36 1 483 4827
E aniko.kircsi@cms-cmck.com

Poland

Małgorzata Urbańska
Partner
T +48 22 520 5597
E malgorzata.urbanska@cms-cmck.com

Romania

Gabriel Sidere
Partner
T +40 21 4073 813
E gabriel.sidere@cms-cmck.com

Ukraine

Nataliya Nakonechna
Senior Associate
T +38 044 391 3377
E nataliya.nakonechna@cms-cmck.com

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

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

1611-0181-4