Data Protection & Privacy 2021

Contributing editors
Aaron P Simpson and Lisa J Sotto

LEXOLOGY
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2012
Ninth edition
ISBN 978-1-83862-322-7

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Data Protection & Privacy

2021

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Lexology Getting The Deal Through is delighted to publish the ninth edition of *Data Protection & Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Canada and Romania.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

LEXOLOGY®
Getting The Deal Through

London
August 2020

Reproduced with permission from Law Business Research Ltd
This article was first published in September 2020
For further information please contact editorial@gettingthedealthrough.com

Contents

Romania

Daniel Alexie, Cristina Crețu, Flavia Ștefura and Laura Dinu
MPR Partners | Maravela, Popescu & Asociații

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The main legislative framework consists of the following:

- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation (GDPR)), directly applicable into the Romanian legislation.
- Law 190/2018 on implementing measures for the GDPR.
- Law no. 102/2005 on the establishment, organisation and functioning of the National Supervisory Authority for Personal Data Processing (DPA).

Guides and recommendations of the European Data Protection Board, as well as guides issued by the DPA must be considered.

Alongside the legislation mentioned above, there are a series of normative acts that are relevant from a data protection perspective, including acts that regulate specific areas of data protection, such as cookies and marketing communication.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The Romanian data protection authority is the DPA.

The DPA is organised as an independent institution. Its powers are based both on the GDPR and on Law no. 102/2005 on the establishment, organisation and functioning of the National Supervisory Authority for Personal Data Processing.

The DPA may conduct investigations, including unannounced ones. During investigations, the DPA may request any documents and information and can access any equipment (including personal data storage equipment) it deems necessary for the purposes of the inspection. The DPA may gather witness statements and commission experts' reports.

Once a breach of legislation has been ascertained, the DPA may impose reprimands or fines, alongside corrective measures. Periodic fines can be imposed in specific cases.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Whenever the activity of the controller or processor of personal data has a cross-border nature, a conflict of competence may arise. The mechanism of solving the conflict of competence is enshrined in GDPR. As a rule, the supervisory authority of the main or single establishment of the controller or processor is competent to act as lead supervisory authority for investigating the cross-border processing carried out by that controller or processor and must cooperate with the other supervisory authorities concerned.

Breaches of data protection

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Under Romanian law, the breaches of data protection law are sanctioned by way of:

- reprimands;
- fines; and
- corrective measures in line with GDPR, in addition the DPA may request the controller and processor to publish at its own cost any of the corrective measures imposed.

An infringement is determined by the control personnel of the DPA and the sanction is applied via a report signed by the same. Where the fine exceeds €300,000, it can be imposed only through a Decision of the President of the DPA, based on the report made by the DPA's control personnel.

The fines are set in the GDPR. These are up to €10 million or up to 2 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher, for infringements regarding, for example, obligations entailed by the privacy-by-design and privacy-by-default principle, security of the processing; and up to €20 million or up to 4 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher, for infringements related to, for example, the basic principles for processing, including conditions for consent, the data subjects' rights.

If there is non-compliance with the imposed measures, or tacit or express refusal to provide all the information and documents requested by the DPA, or if the controller or processor refuses to be subject of an investigation, the DPA may apply a periodic fine of 3,000 Romanian leu per day.

In accordance with the GDPR, Romania decided that a punitive regime should be applicable to public authorities in accordance with the provision of Law No. 190/2018. Therefore, if a public authority infringes GDPR or the national data protection laws, the DPA issues, in

a first phase, a warning accompanied by a remediation plan. The DPA can resume the investigation and if it finds that the measures from the remediation plan were not implemented, a fine ranging from 10,000 to 200,000 Romanian leu might be applied.

Romania decided not to impose criminal penalties for infringements.

SCOPE

Exempt sectors and institutions

5 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The general data protection legal regime enshrined in the General Data Protection Regulation (GDPR) expressly excludes from its scope of application:

- processing of personal data performed during activities outside the scope of European Union Law;
- processing of personal data performed by member states with respect to common foreign and security policy;
- processing of personal data performed by a natural person in the course of a purely personal or household activity;
- processing of personal data performed by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; and
- processing of personal data of deceased persons.

The legal regime of personal data processing is also regulated by other specific pieces of legislation, that cover the processing of personal data in electronic communications, and the processing of personal data while preventing, detecting, investigating, prosecuting and fighting crimes or executing penalties, and education and security measures.

Communications, marketing and surveillance laws

6 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Interception of communications, electronic marketing and monitoring and surveillance of individuals are specifically addressed by the Law No. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector specifically addresses this subject (that transposes into Romanian legislation Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (E-Privacy Directive)). Interception of communications and monitoring and surveillance of individuals is further regulated by the Criminal Procedure Code.

Other laws

7 | Identify any further laws or regulations that provide specific data protection rules for related areas.

Currently, Romania has not developed sector-specific data protection legislation. However, some specific rules (as enabled by the GDPR) are included in the national legislation, regarding the processing of:

- genetic, biometric and health data;
- the national identification number;
- data in employment contexts; and
- data in the context of performing a task that serves a public interest.

These rules do not diverge from the principles and rules of the GDPR.

PII formats

8 | What forms of PII are covered by the law?

The GDPR (and thus applicable national legislation) applies to the processing of personal data wholly or partly by automated means and to the processing, other than by automated means, of personal data which forms part of a filing system or is intended to form part of a filing system, where a 'filing system' means any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or a geographical basis.

Extraterritoriality

9 | Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The GDPR also applies to controllers and processors not established in the European Union when processing activities relate to offering of goods or services to data subjects in Romania, irrespective of whether a payment from the data subject is required; and monitoring of data subjects' behaviour that takes place in Romania.

Also, the GDPR applies to the processing of personal data by a controller not established in the European Union, but in a place where Romanian law applies by virtue of public international law.

Covered uses of PII

10 | Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

Personally identifiable information is not a concept recognised in European law. Therefore, the term to be used is 'personal data'. The GDPR applies where the processing of personal data is done wholly or partly by automated means and where the processing other than by automated means of personal data forms part of a filing system or is intended to form part of a filing system. Processing of personal data covers all the operations, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, erasure or destruction.

All processing activities that are in scope of the GDPR need to observe the rules set in the same.

The majority of obligations and duties sit with the person who determines the purposes and the means of the processing (the controller), as the controller is accountable for the processing activities of the personal data. There are specific obligations and duties that sit also with the person designated by the controller to process data on its behalf (the processor).

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

11 | Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

For any personal data processing activity to be lawful, a legal ground must apply. According to General Data Protection Regulation (GDPR), for general categories of data (eg, name, surname, address, bank account), the processing is lawful when:

- the data subject has consented to the processing;
- it is necessary for the performance of a contract to which the data subject is party or is necessary for taking the steps prior concluding that contract;

- it is necessary for meeting a legal obligation of the controller;
- it is necessary for protecting the vital interests of the data subject or of another natural person;
- is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and
- the controller or a third party has a legitimate interest to process the personal data, save for the case when such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

As regards special categories of data (such as health data, genetic and biometric data, data about political opinions, religious and philosophical beliefs), as a rule, any related processing is forbidden. By way of exception, the GDPR expressly provides in what situations the processing may be carried on, as follows:

- the data subject has expressly given his or her consent;
- the data subject has made public the data;
- for employment, social security and social protection when authorised by law;
- for vital interest;
- for reasons of substantial public interest when law provides;
- for legal claims;
- for health or social care in the public interest when law provides; and
- for archiving, research and statistics in the public interest when law provides.

Legitimate processing – types of PII

12 Does the law impose more stringent rules for specific types of PII?

There are three categories of personal data for which the processing rules differ:

- general personal data;
- special categories of data (eg, race and ethnic origin, religious or philosophical beliefs, political opinions, trade union memberships, genetic data, health data), that have strict rules for processing; and
- personal data for which the GDPR provides that the member states can lay out different regimes (ie, personal identification numbers, health data, processing of personal data in the contexts of employment or fulfilling a task serving the public interest).

If the processing of personal identification number is based on the legitimate interest of the controller or of a third party, Law No. 190/2018 provides that:

- a data protection officer must be appointed;
- appropriate safeguards must be implemented to observe the minimisation principle and to ensure the security and confidentiality of the processing of data;
- a retention period must be set; and
- periodical training for the persons in charge with processing personal data must be conducted.

In respect of genetic, biometric and data concerning the health of the data subject, Law no. 190/2018 provides that processing of such data for profiling or automated decision-making process is allowed only when the data subject has given his or her consent in this respect or if specific legal provisions provides so.

For the processing of personal data in the employment context, Law No. 190/2018 provides that for monitoring (based on legitimate interest) employees through electronic communications or video surveillance , the employer must, among other conditions set by the law, consult with the relevant trade union or representatives of the employees and set a retention period that cannot exceed 30 days, save for the situation when the law provides otherwise.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

13 Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

The General Data Protection Regulation (GDPR) (and consequently, the Romanian legislation) requires the persons collecting data (controllers) to provide data subjects with specific information, at the moment when data is collected – if that data is obtained directly from the data subject or within a reasonable period after obtaining the personal data, but at the latest within one month after obtaining the data – when personal data has not been obtained from the data subject (in this latter case, the data subject can also be notified of the processing at the time of the first communication or when the data is first disclosed to a third party; in both cases, the one month timeframe is observed).

The notification must include information on the following:

1 the identity and the contact details of the controller and, where applicable, of the controller's representative;
2 the contact details of the data protection officer, where applicable;
3 the purposes and legal basis of the processing;
4 where processing is based on a legitimate interest, the legitimate interests pursued by the controller or by a third party;
5 the categories of personal data concerned (when personal data is not obtained from the data subject);
6 the recipients or categories of recipients of the personal data, if any;
7 where applicable, the intention of the controller to transfer the data to a third country or international organisation and the existence or absence of an adequacy decision by the European Commission or, where applicable, the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
8 the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
9 the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing or to object to processing, as well as the right to data portability;
10 the existence of the right to withdraw consent at any time, when the processing is based on consent;
11 the right to lodge a complaint with a supervisory authority;
12 whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
13 the existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and
14 from which source the personal data originates, and if applicable, whether it came from publicly accessible sources (for when the data is not obtained directly from the data subject, in addition to the information mentioned at points (1) to (13) above).

Exemption from notification

14 | When is notice not required?

When the data is obtained directly from the data subject, there is no need inform the data subject of the processing if the data subjects already have the information.

When the data is collected from other sources as the data subject, there is no need to inform the data subject when:

- The data subject already has the information.
- Informing the data subject is impossible or would require a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to various conditions and safeguards provided by the GDPR or as in so far the obligation to inform is likely to render impossible or seriously impair the achievement of the objectives of that practices. In such cases the data controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.
- Obtaining or disclosure of the personal data is expressly regulated by specific legislation and the controller provides safeguards for the data subject's legitimate interests.
- Where the personal data must remain confidential subject to an obligation of professional secrecy, including a statutory obligation of secrecy.

Control of use

15 | Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Data subjects are empowered to exercise control over how their data is being used.

The rights of the data subjects according to the GDPR are:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object;
- the right not to be subjected to an automated decision-making and profiling; and
- the right to lodge a complaint with a supervisory authority.

The rights listed above are not absolute and in many situations the exercise of such rights will be balanced against other competing rights involved. Such competing interests include the right to freedom of expression, the legitimate interests of the controller or of third parties, compliance with legal obligations, and public, scientific, historical or research purposes.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PII?

According to GDPR, the controller must take every reasonable step to ensure that personal data is accurate and up to date (accuracy principle). In this respect, the controller must ensure that the inaccurate personal data, having regard to the purposes for which it is processed, is erased or rectified without delay.

Amount and duration of data holding

17 | Does the law restrict the amount of PII that may be held or the length of time it may be held?

Two principles governed the amount and duration of data holding:

- Data minimisation principle: the collected personal data needs to be limited to what is necessary in relation to the purposes for which is processed.
- Storage limitation principle: the collected personal data must not be kept for longer than necessary for the purposes for which is processed. The GDPR does not set a timeframe for processing. The national legislation provides in some cases for data retention periods (eg, for accounting data 10 years, for employee payment accounting data 50 years).

Finality principle

18 | Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

The GDPR imposes on controllers the obligation to process personal data only for specified, explicit and legitimate purposes and not in a manner that is incompatible with those purposes (the Purpose Limitation principle).

The processing of personal data for other purposes than those for which the personal data was initially collected is allowed where:

- it is based on the data subject's consent;
- it is based on the laws of the European Union or a member state; or
- where the processing is compatible with the purposes for which the personal data was initially collected.

Use for new purposes

19 | If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The GDPR correspondent for the finality principle is the 'purpose limitation' principle. According to it, personal data may only be collected for specified (defined), explicit (clear) and legitimate purposes (legal basis) determined at the moment of collection.

Further processing activity is allowed if the personal data is processed for:

- Archiving, scientific, historical or statistical purposes as far as appropriate technological and organisational measures are in place to protect the rights and freedoms of the data subjects, in particular, the principle of data minimisation.
- Another purpose compatible with the purpose for which the personal data was initially collected. A compatibility test is required in this case. When assessing the compatibility, the controller should consider:
  - the relationship between the purposes for which the personal data was collected and the further processing purpose;
  - the reasonable expectations of the data subject, as to the further use of his or her personal data; and
  - the nature of the personal data, the possible consequences for data subjects, and the existence of appropriate safeguards (such as encryption and pseudonymisation).

SECURITY

Security obligations

20 What security obligations are imposed on PII owners and service providers that process PII on their behalf?

Under the 'integrity and confidentiality' principle, the data controllers are required to process personal data in a manner that ensures appropriate security of the data. This covers protection against unauthorised or unlawful processing, and accidental loss, destruction or damage by implementation of appropriate technical and organisational measures. Both controllers and processors are responsible for implementation of appropriate technical and organisational measures in order to process personal data in a secure manner. A case-by-case risk assessment is needed.

Notification of data breach

21 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The regime of data breach notifications is regulated by General Data Protection Regulation (GDPR) and it is applicable across all industries. Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector (Electronic Communications Law) imposes a sector-specific duty to notify personal data breaches, applicable only for the electronic communications service providers.

In both cases, the notification must be submitted to the National Supervisory Authority for Personal Data Processing (DPA), with the mention that under the GDPR the timeframe for submission is 72 hours since becoming aware about the incident, while under the Electronic Communications Law the notification must be submitted in 24 hours since finding about the incident.

The threshold for notification under the GDPR is a risk-based one. The controller must submit the notification to the DPA when it is likely that the personal data breach will create a risk to the rights and freedoms of natural persons. Also, in what concerns the communication to the data subject, the controller must notify the same about the data breach when it is likely that the data breach will result in a high risk for the data subject.

Based on Electronic Communication Law, all data breaches covered by the law must be notified to the DPA. In addition, as a rule, the electronic communications provider must also notify the subscriber about the incident when the data breach could affect the personal data or privacy of a subscriber or another person, save for the case when the electronic communication provider is able to demonstrate in a manner that the DPA finds satisfying that appropriate measures for the protection of the personal data affected by the incident have been implemented.

INTERNAL CONTROLS

Data protection officer

22 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

As per General Data Protection Regulation (GDPR), there are three situations in which the appointment of a data protection officer (DPO) is mandatory, as follows:

- when the processing is carried by a public authority or body (including government departments);
- where the core activities of the controller or processor consists of data processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions or offences.

However, the National Supervisory Authority for Protection of Personal Data (DPA) expressly recommends the appointment of a DPO also in those cases when it is not mandatory to appoint such, considering the beneficial role that the DPO may play in ensuring the observance of the GDPR's provisions by the controller or processor. The Article 29 Working Party also recommends that, save for the situation where it is obvious that the designation of a DPO is not mandatory, the internal assessment to determine if a DPO is to be appointed needs to be documented, in line with the accountability principle.

As per Law no. 190/2018, the appointment of a DPO is mandatory when a controller decides to process personal identification numbers based on legitimate interest.

The DPO's responsibilities are the following:

- informing and advising the controller, processor or their employees on their duties arising from the data protection legislation;
- monitoring compliance with GDPR, the national data protection legislation, and the data protection related policies of the controller or processor, including carrying out the related audits;
- the assignment of responsibilities, awareness raising, and training of staff tasked with personal data processing;
- providing advice, where requested, regarding the data protection impact assessments and monitoring the performance of the same; and
- cooperation with and acting as contact point for the DPA.

Record keeping

23 Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

The GDPR introduced, for both the controllers and processors, the obligation to keep records in writing, including in electronic form, of the processing activities under their responsibilities.

The controller needs to keep a registry with the following information:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the DPO;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom personal data has been or will be disclosed;
- transfers of personal data to a third country or an international organisation;
- the envisaged time limits for erasure of the different categories of data; and
- a general description of the technical and organisational security measures in place.

The processor needs to keep a registry with the following information:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the DPO;
- the categories of processing carried out on behalf of each controller;

- transfers of personal data to a third country or an international organisation, and safeguards implemented for such transfers; and
- a general description of the technical and organisational security measures in place.

Companies with less than 250 employees are exempted from this obligation, save for the cases when the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or data related to criminal convictions or offences. More information on the derogations are set in the position paper published by the Article 29 Working Party.

New processing regulations

24 | Are there any obligations in relation to new processing operations?

Embedding privacy-by-design and privacy-by-default are now both legal requirements under the GDPR. Moreover, not ensuring the implementation of the same represents an infringement of the GDPR and is a criterion considered by the National Supervisory Authority for Personal Data Processing (DPA) when assessing whether to impose an administrative fine. Thus, the controller, regardless of the type of data processed or the nature of the processing, has the duty to implement appropriate technical and organisational measures (such as pseudonymisation, data minimisation, enabling the data subject to monitor the data processing) from the moment of determining the means for processing and at the time of the processing itself. In addition, the controller needs to ensure that only the data that are necessary for each specific purpose of the processing are processed.

The controller has also a duty to carry a data protection impact assessment prior to a personal data processing activity that is likely to result in a high risk to the rights and freedoms of the data subjects. Such risk could be physical, material or non-material. Building on the cases expressly mentioned by the GDPR, the DPA issued a decision which comprises a list of cases in which the data protection impact assessment is required (eg, in the case of a systematic monitoring of a systematic monitoring of a publicly accessible area on a large scale, such as video surveillance in malls, stadiums, parks, plazas, or other similar places). This is a non-exhaustive list.

REGISTRATION AND NOTIFICATION

Registration

25 | Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

In Romania, no obligation of registration with the national DPA exists since the General Data Protection Regulation (GDPR) became applicable on 25 May 2018.

Formalities

26 | What are the formalities for registration?

Not applicable.

Penalties

27 | What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Not applicable.

Refusal of registration

28 | On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable.

Public access

29 | Is the register publicly available? How can it be accessed?

Not applicable.

Effect of registration

30 | Does an entry on the register have any specific legal effect?

Not applicable.

Other transparency duties

31 | Are there any other public transparency duties?

The GDPR imposes on controllers the transparency obligation towards the processing activities and they are obliged to demonstrate compliance with it.

The transparency principle mandates to provide, in writing, or by other means, including, where appropriate, by electronic means, relevant information to data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

32 | How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Under the General Data Protection Regulation (GDPR), the concept of transfer implies that personal data is transmitted from a controller or processor located in the European Economic Area (EEA) to international organisations, controllers, processors or other recipients located outside the EEA. Otherwise, the transmission of personal data to a provider of processing services that is located in EEA will be regulated by a contract or other binding act, depending on its qualification as a processor, controller or joint controller in relation to the processed personal data and does not imply a transfer in the sense of the GDPR.

Restrictions on disclosure

33 | Describe any specific restrictions on the disclosure of PII to other recipients.

There are no specific restrictions regarding the disclosure of personal data to other recipients.

Cross-border transfer

34 | Is the transfer of PII outside the jurisdiction restricted?

The cross-border transfer of personal data between controllers or processors located in the EEA is permitted without restriction. However, for cross-border transfers outside the European Union and EEA (either to a third country or to an international organisation), as a rule, the transfer of personal data is not allowed, save for the following situations:

- based on an adequacy decision issued by the European Commission, providing that the third country has implemented safeguards that ensure the protection of personal data and of the rights and freedoms of the data subjects; and

- based on appropriate safeguards implemented by the controller or processor that transfers the personal data.

Some examples of appropriate safeguards include binding corporate rules, standard data protection clauses adopted by the European Commission or adopted by a supervisory authority and approved by the European Commission. In cases where the appropriate safeguards are provided through simple contractual clauses, an authorisation from the competent National Supervisory Authority for Protection of Personal Data (DPA) is mandatory.

Notification of cross-border transfer

35 | Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

When the personal data is transferred to a recipient located outside the EEA, based on an agreement between the sender and the recipient, the contractual clauses regulating the transfer are subject to a specific authorisation issued by the DPA. Also, the administrative arrangements between public authorities or bodies are subject to an authorisation issued by the DPA.

Further transfer

36 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Yes, the restrictions are applicable for any type of transfer, as regulated by the GDPR, irrespective of the quality of the recipient. As for onward transfers, the same conditions under which the first transfer was made must be also applied for the onward transfer, so that the same level of protection is ensured.

RIGHTS OF INDIVIDUALS

Access

37 | Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

The data subject has the right to a confirmation on whether the controller processes his or her data, and to access that information.

The data subject is entitled, upon specific request, to a copy of the personal data that is processed. Further copies can be subject to a reasonable fee by the controller. That right shall not adversely affect the rights and freedoms of others.

The controller must also provide a list of details that replicates the information that needs to be provided under the transparency obligation (article 13 and 14 from General Data Protection Regulation (GDPR)).

Other rights

38 | Do individuals have other substantive rights?

Other substantive rights of the data subject, apart from the access right, are:

- the right to information (ie, the right to be informed of the processing);
- the right to rectification (ie, the right to rectify any inaccuracies in the processed data);
- the right to be forgotten (ie, the right to erasure of the processed data, in certain conditions);
- the right to restriction (ie, the right to obtain the restriction of the processing of data, in certain conditions);
- the right to data portability (ie, the right to receive from the controller the personal data concerning the data subject in a structured and machine-readable format to transmit those data to another controller, subject processing activities have as a legal base a contract with or the consent of the data subject and they are carried out by automated means);
- the right of objection (ie, the right to oppose the processing, in certain conditions);
- the right not to be subjected to an automated decision-making (ie, the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or adversely affects the data subject); and
- the right to lodge a complaint with a supervisory authority.

Compensation

39 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The GDPR provides for an effective judicial remedy, as well as for compensation, whenever the rights of data subjects have been breached.

In Romania, monetary compensation is available for both material and moral damages. However, the award of monetary compensation for moral damages is to be granted by a court of law following a substantiated request to this end submitted by the affected data subject.

Enforcement

40 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The rights of the data subjects can be enforced by the DPA or directly through effective judicial remedies when the data subjects consider that their rights have been breached.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

41 | Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

In Romania, the law implementing the General Data Protection Regulation (GDPR) provides for derogations for processing of data for journalistic purposes or for the purpose of academic, artistic or literary expression, as well as for scientific or historical research purposes, artistic or public archiving purposes.

Processing for journalistic purposes or for the purpose of academic, artistic or literary expression may be carried out if it concerns personal data that has been manifestly made public by the data subject or which is closely linked to the data subject's capacity as a public person or the public nature of the facts in which it is involved, without the applicability of specific chapters from the GDPR, such as, among other things, the chapters regarding the principles, the rights of the data subjects and others.

Certain rights of the data subject provided by the GDPR will not apply where personal data is processed for scientific or historical research purposes, for statistical purposes (ie, namely rights to access; to rectification; to restriction of processing; and to object) or archiving purposes in the public interest (ie, namely right of access; to rectification; to restriction of processing; to notification; to be informed as regards any rectification, erasure of personal data or restriction of processing; to data portability; and to object), in so far as these rights make it impossible or seriously affect the achievement of the specific objectives, and such derogations are necessary for the fulfilment of those purposes.

The derogations mentioned above apply only where the processing is subject to appropriate safeguards, in accordance with the GDPR.

SUPERVISION

Judicial review

42 | Can PII owners appeal against orders of the supervisory authority to the courts?

Against the minutes of finding or sanctioning a breach of the personal data protection legislation, or against the decision to apply corrective measures, issued by the National Supervisory Authority for Protection of Personal Data (DPA), the controller or the processor can file a complaint with the competent tribunal, within 15 days from when that decision was delivered or communicated.

SPECIFIC DATA PROCESSING

Internet use

43 | Describe any rules on the use of 'cookies' or equivalent technology.

Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector (Electronic Communications Law), transposed in the Romanian legislation the Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (E-Privacy Directive) regulates the use of cookies. Related to cookies, the Electronic Communications Law provides two cumulative conditions for storing information or gaining access to information stored in the terminal equipment of a subscriber or user, as follows:

- the subscriber or user has given his or her consent; and
- prior to giving consent, the subscriber or user has been provided with clear, complete, and easy to understand information related to the purposes of the processing.

Electronic communications marketing

44 | Describe any rules on marketing by email, fax or telephone.

The regime for marketing by electronic communications means is regulated by the Electronic Communications Law that transposed in the Romanian legislation the E-Privacy Directive. Sending marketing communications using automated means that do not require human intervention, such as through fax or electronic mail or any other method that uses electronic communication services aimed at the public is not permitted if the user or the subscriber has not expressly given his or her prior consent in this respect. As an exception, where a natural or legal person obtains, in the context of the sale of a product or a service, the electronic mail address of its customers their electronic mail address, the same natural or legal person may use these electronic mail address for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such receiving at the time of their collection and on the occasion of each message, in case the customer has not initially refused such use.

MPR PARTNERS
MARAVELA, POPESCU & ROMAN

Daniel Alexie
daniel.alexie@mprpartners.com

Cristina Crețu
cristina.cretu@mprpartners.com

Flavia Ștefura
flavia.stefura@mprpartners.com

Laura Dinu
laura.dinu@mprpartners.com

6A Barbu Delavrancea Street
Building C, Ground Floor
1st District
Bucharest 011355
Romania
Tel +40 21 310 17 17
www.mprpartners.com

Cloud services

45 | Describe any rules or regulator guidance on the use of cloud computing services.

The cloud computing service is defined under Law no. 362/2018 concerning measures for a high common level of security of network and information systems which transposes into national legislation Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). However, the Romanian law does not provide specific rules applicable to cloud computing services.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

In the past year, the activity of the National Supervisory Authority for Protection of Personal Data (DPA) became more intense and the first fines following the infringement of General Data Protection Regulation (GDPR) have been applied. As a summary, in 2019, the DPA received a total of 6,193 complaints, petitions and personal data breaches notifications, based on which 912 investigations were opened. Pursuant to the investigations, 28 fines were issued in a total amount of 2,339,291.75 Romanian leu. In addition, 134 reprimands and 128 corrective measures have been applied. A significant number of fines have been applied for the infringement of article 32 of GDPR that obliges the controllers and processors to implement technical and organisational measures appropriate to the risk of processing. Also, several fines have been issued for not observing the rules for lawfulness of processing, the rules concerning the rights of data subjects and for infringement of privacy-by-design and privacy-by-default provisions.

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-322-7