Personal Data Protection

LEGISLATIVE AND REGULATORY FRAMEWORK

1. What is the relevant legal framework? Are there any pending legislative amendment proposals?

Primary legislation

The general legal framework governing data privacy has changed substantially once Regulation (EU) 2016/679 (GDPR) came into force on 25 May 2018.

In consideration of the so-called GDPR "opening clauses", Romania has enacted implementation legislation, namely:

- Law No. 190/2018 on measures to implement GDPR, setting forth special rules for the processing of certain categories of personal data, certain derogations from GDPR, certain special rules regarding the data protection officer and certification bodies, as well as certain derogations from sanctions applicable with respect to public and private entities. Law No. 190/2018 has been amended by Law No. 233/2019 introducing statistical purposes on the list of derogations from Articles 15, 16, 18 and 21 of GDPR;
- Law No. 129/2018 amending and supplementing Law No. 102/2005 regarding the setting up, organisation and functioning of the National Supervisory Authority for Personal Data Processing (DPA), comprising the rules on the organisation and functioning of the DPA;
- Law No. 284/2018 on the use of PNR (passenger name records) data for the prevention, detection, investigation and prosecution of terrorism offenses and serious crime, as well as for the prevention and elimination of threats to national security;
- Law No. 363/2018 on the implementation of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such

data, and repealing Council Framework Decision 2008/977/JHA;

- Law No. 362/2018 on the implementation of NIS Directive 2016/1148 ensuring a high common level of security of computer networks and systems with regard to preventing, detecting and reacting to cyber-security breaches and the list of entities considered "operators of essential services" and subsequent methodological norms. Law No. 362/2018 has been amended by the Government Emergency Ordinance No. 119/2020 transferring the power to establish and submit to the Government's approval (i) the threshold values for determining the significant disruptive effect of incidents on the networks and computer systems of essential service operators and the (ii) thetechnical rules for determining the impact of incidents from the Ministry of Communications and Information Society to the National Cyber Security Incident Response Center (CERT-RO) and the Interinstitutional Working Group;
- Law No. 209/2019 on payment services and the aendemnt of other enactments, implementing the Payment Services Directive ('PSD2'), regulation the conditions of access to the activity of providing payment services, the prudential supervision of payment institutions and specialised providers of information services regarding accounts, the transparency regime for conditions and information requirements regarding payment services, as well as the corresponding rights and obligations of payment service users and payment service providers;
- Law No. 129/2019 implementing the AML Directive ((EU) No. 849/2015), regulating know-your-customer measures.

Aside from this new legislation, there are still some relatively old data privacy legal norms governing specific sectors, such as Law No. 365/2002 on electronic commerce and Law No. 506/2004 on the processing of personal data and protection of private life in the sector of electronic communications.[1]

Furthermore, as of 26 June 2020, Romania had signed the Council of Europe Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+).

Secondary legislation

The DPA has issued the following secondary enactments addressing essential GDPR aspects:

- DPA Decision No. 128/2018 on the approval of the form of the notification of a personal data breach in accordance with GDPR;[2]
- DPA Decision No. 133/2018 on the approval of the procedure for receiving and

1 The E-Privacy Law implements Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

2 http://www.dataprotection.ro/servlet/ViewDocument?id=1516.

handling complaints;[3]
- DPA Decision No. 161/2018 on the approval of the procedure for conducting investigations;[4]
- DPA Decision No. 174/2018 on the approval of the cases in which a data privacy impact assessment is mandatory;[5]
- Methodological Norms implementing Law No. 362/2018;
- Government Decision No. 963/2020 for the approval of the List of essential services;
- Government Decision No. 976/2020 on the approval of threshold values for establishing the significant disruptive effect of incidents on the networks and computer systems of essential service operators.

Upcoming national legislation in data privacy sector

As for pending proposals of enactments, we note the following draft regulations:

- E-Privacy Regulation;
- Draft law on electronic identification and trust services for electronic transactions in the internal market, sent for report to the Permanent Commissions of the Parliament;
- Draft law on repealing Articles 6 and 9 of Law No. 190/2018. Article 6 of Law No. 190/2018 covers the processing of personal data and special categories of personal data in the context of a public service task. Article 9 of Law No. 190/2018 covers the safeguards for the processing of personal data by political parties and citizens' organizations belonging to national minorities and non-governmental organizations. This draft law enjoys the support of the Romanian DPA, according to its annual report for 2019;[6]
- Draft law on enforcing public authorities' obligation to provide personal data processed in respect to the data subject making the request, adopted by the Senate but not yet promulgated;
- Draft law on amending Law No. 362/2018 on the implementation of NIS Directive 2016/1148 ensuring a high common level of security of computer networks and systems with a view to preventing, detecting and reacting to cyber-security breaches and the list of entities considered "operators of essential services" and subsequent methodological norms, adopted by the Senate but not yet promulgated;
- Romanian DPA Draft Decision establishing additional requirements for the accreditation of certification bodies pursuant to Article 43 of the GDPR.[7]

3 http://www.dataprotection.ro/servlet/ViewDocument?id=1517.

4 http://www.dataprotection.ro/index.jsp?page=control&lang=en.

5 http://www.dataprotection.ro/servlet/ViewDocument?id=1556.

6 Such is available at: https://www.dataprotection.ro/?page=Rapoarte%20anuale&lang=ro.

7 Such is available in Romanian or English at: https://www.dataprotection.ro/index.jsp?page=Proiect_decizie_criterii_certificare_ANS&lang=en.

Guidelines

The Romanian DPA issued a Guideline comprising punctual clarifications for controllers, processors and natural persons regarding the application of the provisions of GDPR, of Law No. 190/2018 and of the decisions issued by the Romanian DPA[8].

2. Which is the relevant authority in data protection field?

The local authority with overall competences in data protection field is the Romanian Authority for Personal Data Protection and Supervision – DPA.[9]

3. Which entity is the national accreditation body named in accordance with Regulation (EC) No. 765/2008 of the European Parliament and of the Council (1) in accordance with EN-ISO/IEC 17065/2012?

Currently, the national accreditation body recognised by Law 190/2018 is the Romanian Accreditation Association – RENAR.

Certification Bodies will be accredited according to applicable legal regulations in accordance with EN-ISO / IEC 17065 and with the additional requirements set by the DPA, as well as with the provisions of Article 43 of GDPR.

LOCAL PARTICULARITIES

1. What are the DPA's investigation powers in Romania?

The DPA's inspection staff is entitled to:

- Carry out investigations, including on-the-spot;
- Request and obtain from the controller and the person authorised thereby and, where appropriate, from their representative, on the spot and/or within a specific time frame, any information and documents, regardless of the storage medium;
- Retrieve copies of any requested information;
- Have access to any premises of the controller and the person authorised by the

8 Such is available in Romanian only at: https://www.dataprotection.ro/?page=Comunicat_lansare_ghid_intrebari_si_raspunsuri&lang=ro.

9 The official website of the DPA is http://www.dataprotection.ro.

controller;
- Have access to and verify any equipment, medium or data storage medium, necessary for carrying out the investigation, according to the law;
- Conduct audits and hearings of persons whose statements are considered relevant and necessary for the investigation; and
- Conduct audits onsite, at the headquarters of the DPA or via written correspondence.

Where its access to information is not granted or otherwise hindered, the DPA may obtain judicial authorisation to proceed with the control.

2. How can a complaint be submitted with the DPA?

Complaints can be filed by any person who considers that the processing of his/her personal data is unlawful, particularly if their habitual residence, place of work or place of the alleged violation is located, or occurs within the territory of Romania.

The following key rules should be considered when filing complaints with the DPA:[10]

- Form and content:
  - Must be written in Romanian or English;
  - Must provide the full identification data of the petitioner and, where the case, of the person authorised by the petitioner;
  - Must provide full identification data of the controller or its proxies;
  - Shall be signed in physical or electronic form, and in the case of petitions sent electronically that cannot be signed, the DPA may request confirmation of the accuracy of the electronically transmitted data;[11]
  - Must indicate a detailed description of the object of the complaint, actions taken by the petitioner in relation to the controller or its representatives, the state of facts and arguments supporting the allegations, as well as all related supporting documentation.
- Rules for submission:
  - May be submitted either to the general registry at the DPA or may be sent by post, including electronic mail, or by use of the electronic form available on the DPA website;
  - May be filed by the petitioner or its legal/ authorised representative or via a body, an organisation, association or non-profit foundation active in the field of protection of the rights and freedoms of data subjects.

10 Either by using the standard form provided within Annex 2 of DPA Decision No. 133/2018 or by filling a separate form.

11 The complaints may be sent in electronic form at *plangere@dataprotection.ro*.

The petitioners may expressly request the confidentiality of personal data, except where, for the proper settlement of the lodged complaints, the petitioner's identification data must be disclosed to the defendant.

As a rule, submission of complaints is free of charge. By exception, the DPA might apply a reasonable administrative fee or even refuse to assess the complaint where such is clearly unfounded or excessive.

Where a legal action is brought before the court in respect of the same subject matter, the DPA may order the suspension and / or quash the complaint, as appropriate. Legal actions before courts are free of any stamp duties.

3. Are there any national rules governing the security breach topic?

Currently, the national legislation does not address any specific rules on the security breach matter. Therefore, the general rules prescribed by GDPR shall apply accordingly.

Nevertheless, the DPA has published on its website a template form for security breach notifications. The form can be signed and lodged electronically with the DPA, to a dedicated e-mail address - *brese@dataprotection.ro* or submitted in physical counterpart to the DPA.

4. Are there any special requirements for being a local DPO?

The DPO must have appropriate knowledge to fulfil the data privacy tasks specific to such position within the organisation. In this respect, the DPA has ruled that the DPO must:

- Have expertise in data protection legislation and practices at national and EU level;
- Have the necessary level of knowledge in the field of data protection, depending *inter alia* on the type of data processing operations performed within the organisation and the level of protection required for processed personal data;
- Understand the processing operations carried out, as well as information systems and security and data protection needs;
- In the case of a public authority or institution, it must also have knowledge of the legal regulations of organisation and their activity, as well as the internal administrative procedures for the deployment activity.

The DPO may hold another position within the controller and thus carry out other

tasks than those in relation to his/her position, provided that such do not generate any conflict of interest. For instance, the DPO cannot hold the position of executive director, operational director, Chief Financial Officer, Head of Medical Service, Head of Marketing, Head of the Human Resources department or Head of the IT department within the organisation.

5. How do you notify the DPO with the DPA?

The DPA has made available on its website a standard form for DPOs notification. The notification must be filled in and submitted via the DPA website (at *https://www.dataprotection.ro/formulare/formularRpd.do?action=view_action&newFormular=true*).

6. Are there any local rules addressing the processing of employees' personal data?

Local legislation provides for special rules to be observed when monitoring the employees by electronic communication means or via CCTV at the workplace based on the *legitimate interest* of the controller.

As per such rules, the monitoring may occur only where:

- The *legitimate interests* pursued by the controller (employer) are well grounded and override the interests, rights and freedoms of targeted data subjects (employees);
- The employer provided the employees with comprehensive and overt information before the surveillance occurred;
- The employer consulted the trade union or the employees' representatives before introducing the means of surveillance;
- Other less intrusive forms and modalities did not prove their efficiency, considering the envisaged purpose of the surveillance;
- The data resulted from surveillance may be kept for a maximum of 30 days, except where the law provides otherwise, or a well-grounded reason justifies such processing.

7. Are there any local rules on data protection impact assessments (DPIA)?

As per the local legislation, performing a DPIA is mandatory when:

- Processing has as purpose a systematic and comprehensive assessment of personal

information relating to individuals, which is based on automatic processing, including the creation of profiles, and which is the basis for decisions that produce legal effects on the individuals or have significant similar effects on the latter;

- There is a large-scale processing of data revealing racial or ethnic origin, political opinions, faith denomination or philosophical beliefs or membership to trade unions, genetic data, biometric data for the sole identification of an individual, health data, sexual life or sexual orientation of an individual or personal data related to criminal convictions and offenses;
- Processing has as purpose the systematic surveillance on a large scale in an area accessible to the public, such as CCTV surveillance in public areas (shopping centers, stadiums, markets, parks or other such areas);
- There is a large-scale processing of personal data of vulnerable persons, particularly minors and employees, via automated means and/or systematic recording of behavior, including for advertising and marketing purposes;
- There is a large-scale processing of personal data via innovative use or implementation of new technological solutions, particularly where the processing operations limit the ability of data subjects to exercise their rights, such as the use of facial recognition techniques to facilitate access to different spaces;
- There is a large-scale processing of data generated by devices with sensors that transmit data over the Internet or other means ("the Internet of Things", such as smart TV, connected vehicles, smart meters, smart toys, intelligent cities or other such applications);
- There is a large-scale and/or systematic processing of location or tracking data of individuals (such as Wi-Fi tracking, geographic location data processing of public transport passengers or other such situations) where processing is not necessary for the provision of a service requested by the data subject.

By exception, the DPIA is not mandatory where the processing carried out under Article 6 (1) (c) or (e) GDPR is based on EU or national law, and an impact assessment on data protection has already been carried out as part of a general impact evaluation in the context of the approval of normative enactments.

The DPA has not yet issued a list of activities that are not subject to DPIA.

8. How can a DPA decision be challenged and what deadlines are applicable in this respect?

DPA sanctioning minutes or decisions providing for corrective measures may be challenged at the administrative section of the competent tribunal within 15 days as of receipt of the minutes or communication of the decisions.

The decision on the challenge is also subject to appeal.

The challenging of DPA enactments only leads to automatic suspension with regards to the payment of the fine.

Where the controller also wants to suspend the corrective measures (data erasure, the suspension of the processing operations), a specific application for suspension must be filed with the court.

9. Is there a local statutory time bar applicable in case of data protection misdemeanours?

The DPA may apply a fine or a warning within three years as of the date the misdemeanour takes place. Where the misdemeanour takes place over a prolonged period of time, the limitation period starts as of the end of the last act or fact, if such occurs after the moment when the misdemeanour is ascertained.

The limitation period can be interrupted by undertaking any procedural act, without exceeding four years as of the occurrence of the misdemeanour.

10. Are there any local special derogations from GDPR?

Main local derogations from GDPR:

- Data processing for journalistic purposes or for academic, artistic or literary expression, provided that it refers to personal data that were expressly made public by the data subject or which are strictly related to the status of public figure of the data subject or to the public character of the facts that person is involved in, may be undertaken by derogation from the following chapters of the GDPR: Chapter II - Principles; Chapter III – Rights of the data subject; Chapter IV – Controller and processor; Chapter V - Transfers of personal data to third countries or international organisations; Chapter VI – Independent supervisory authorities; Chapter VII – Cooperation and consistency; and Chapter IX - Provisions relating to specific processing situations;
- Processing personal data for scientific, historical research or statistical purposes are exempted from the provisions of Articles 15, 16, 18 and 21 of the GDPR, in so far as such rights mentioned in these articles, given their nature, render impossible or seriously impair the achievement of the specific purposes and those derogations are required for the fulfilment of these purposes;
- Processing of personal data for archiving purposes in the public interest are

exempted from the provisions of Articles 15, 16, 18, 19, 20 and 21 of the GDPR, in so far as such rights mentioned in these articles, given their nature, render impossible or seriously impair the achievement of the specific purposes and those derogations are required for the fulfilment of these purposes.

In the latter two mentioned derogation cases, appropriate guarantees for the rights and freedoms of data subjects should be considered as provided under Article 89 para. (1) of GDPR.

- Under Law No. 284/2018: (i) particular technical measures are imposed to air carriers; (ii) supplementary requirements are provided for the DPO of the national information unit (UNIP) handling PNR data; (iii) derogations are made for limited purposes for third countries transfers; (iv) processing PNR data by processors is forbidden; (v) the processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, sex life or sexual orientation is prohibited and if UNIP receives these categories of data, such will be erased; (vi) the PNR data is stored for a period of 5 years in the national data records system and depersonalized after 6 months from submission to such system; (v) particular traceability rules are provided; (vi) UNIP must notify any security breaches susceptible of risks for data subjects within 24 hours as of acknowledgement, and if not possible, within 72 hours with justification for the delay in notification (under GDPR, the rule is the 72-hours time frame).
- Under Law No. 362/2018 and subsequent enactments, supplementary obligations are regulated for the operators of essential services and digital services providers[12], such as: (i) need to implement particular security and technical measures and audit controls for the network and information systems and the digital data within, including for personal data processing; (ii) need to also notify, without delay, the breaches that have a significant impact on network security, to CERT RO (national cyber security and incident response team);
- Under Law No. 363/2018, when personal data are processed by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, particular derogations from GDPR are applicable (with the mention that GDPR does not apply to the processing undertaken under such framework), such as: (i) the use of automated individual decision-making, including profiling is allowed only where the law expressly provides such, including the adequate safeguard for such type of operations; (ii) the time limit for replying to the data subjects requests is 60 calendar days; (iii) joint controllers are designated by law (which also establishes the purposes and means of such processing); (iv) appointment of a sub processor

12 Determined in accordance with the provisions of Ministry of Communications and Information Society Order No. 599/2019 regarding the approval of the Methodological Norms for the identification of the essential service operators and digital service providers and Order No. 601/2019 for the approval of the Methodology for establishing the significant disruptive effect of incidents on the networks and information systems of the essential service operators.

is allowed only with the prior written approval of the competent authority; (v) the competent authorities and their processors are obliged to keep adequate pre-defined logs for all data processing operations; (vi) the prior consultation of the Romanian DPA is mandatory when the envisaged processing operations entail a high risk in respect of the rights and freedoms of data subjects; (vii) where the security breaches present high risks, competent authorities must notify concerned data subjects within a maximum of 10 calendar days as of the moment they notify the Romanian DPA about such incidents (under GDPR, no such time limit is provided).

11. Local practice

The Romanian DPA has published its activity report for 2019[13] and a summary of its activity in 2020.[14] Such documents refer, *inter alia*, to the opinions of the Romanian DPA on specific data processing operations, its audit and sanctioning activity and its regulatory activity.

13 Such is available only in Romanian at: https://www.dataprotection.ro/?page=Rapoarte%20anuale&lang=ro.

14 Such is available only in Romanian at: https://www.dataprotection.ro/index.jsp?page=Comunicat_Presa_11_02_2021&lang=ro.