

A N N A K A C Z Y Ń S K A

§

RADCA PRAWNY

CONSEILLER JURIDIQUE

LEGAL ADVISER



Modified controllers and processors obligations under the General Data Protection Regulation (GDPR) from the challenge for the lawyer point of view.

1. Configurations of lawyers possible interventions as regards new controllers'/processors' obligations,
2. Areas of changes in controllers/processors obligations,
3. Extra-territorial scope of GDPA and modifications in relations between controller and processor - contracting to process personal data
4. Specificity of the GDPR (text, notion, structure) to take into consideration while analysing new controllers'/processors' obligations.

Data protection in lawyer's practice:

- providing legal support to a controller or to a processor from EU country, or to a processor seated from outside of the EU, both in public and in private sector,
- lawyer as a controller in her or his own legal office conducted as a business activity,
- representing data subjects defending individuals's private life and human rights

Areas of changes in controllers/processors obligations:

1. Expanded territorial reach,

Art.. 3 (2) Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

- 2. Introduction of the obligations also on data processors,**
- 3. New obligations connected with obtaining a consent, and in connection with a particular protection of children,**
- 4. Right to be forgotten – in other words right to erasure,**
- 5. Right to data portability,**
- 6. Information obligations, including those concerning profiling,**

- 7. Data protection by design and by default standards,**
- 8. Carrying out data protection impact assessment,**
- 9. Records of data processing,**
- 10. Rules of appointing data protection officer,**
- 11. Data breach notifications,**
- 12. Modified rules of data transfers outside the EU,**

13. New obligations as for the contracts to process personal data between controller and processor.

,processing' - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4 (2))

,controller' - the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines **the purposes and means of the processing of personal data**; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (Article 4 (7)),

,processor' - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; (Article 4 (8)).

Recital 81) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, **when entrusting a processor with processing activities**, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be **governed by a contract or other legal act under Union or Member State law**, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use **an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission**. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.

These rules are set out and precised in art. 28-29 GDPR

The obligations of processor - overview:

- stated in art. 27 to appoint a representative if based outside of the Union,
- art. 28 (3) to ensure certain minimum provisions in contracts with controllers,
- art. (28 (2), (4) not appoint sub-processor without specific or general authorisation of the controller and to ensure there is a contract with that sub-processor that contains minimum provisions introduced by the Regulation,
- art. 29 process the data only on the instructions of the controller unless required to do it for other purposes by Union and Member State law,
- art. 30 to keep record of processing carried out on behalf of a controller,
- art. 31 the cooperation with the supervisory authorities,
- art. 32 to implement appropriate security measures,
- art. 33 (2) notification to the controller of any personal data breach without undue delay
- art. 37 to appoint a data protection officer if applicable,
- art. 44 to comply with the rules on transfer of personal data outside of the EU

Specificity of the GDPR (text, notion, structure) to take into consideration while analysing new controllers'/processors' obligations.

Full harmonisation ? Problem of national divergences

Most important areas of national derogation that should be included into analysis while analysing new controller/processor obligations:

1. Differences in processing in the context of employment, Article 88
2. individuals' rights under the Regulation can be limited in the field of national security, crime, and judicial proceedings, Article 23

3. Amendments to reconcile data protection values with freedom of information, in order to protect information subject to professional secrecy and to restrict the processing of national identity numbers Articles 85-91

It covers such areas as processing for journalistic purposes and the purposes of academic, artistic or literary expression, public access to official documents, processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, adopting specific measures in relation to controllers or processors that are subject to an obligation of professional secrecy, data protection rules of churches and religious associations

4. As regards designation of DPO- Member States can decide that the appointment of a data protection officer will be mandatory Article 37 paragraph (4),

5. The age at which they can provide valid consent online may be reduced from 16 to 13, Article 8,

6. Article 6 (1)c as regards controllers lawfulness of processing states that the compliance with an obligation under Union or Member State law is one of the justification of data processing,

7. The information about criminal offences can be processed only if it is authorised by Union or Member State law or under the control of an official authority, Article 10

8. The right to be forgotten does not apply if the processing is necessary for compliance with a legal obligation under Union or Member State law,

Article 17

9. According to art. 49 (4) and (5) Member States may introduce additional restrictions on transfers outside of the EU and on the other hand, a public interest recognised under Member States law can constitute a basis to such a transfer.

What else should we take into consideration while working with the act and specifying in our case the exact controllers/processors obligations?

- often principle-base character of certain concepts in GDPR

- relation articles- recitals

Thank you for your attention

Kancelaria Radcy Prawnego Anna Kaczyńska
Al. Tadeusza Kościuszki 59/61 lok. 410
90-514 Łódź

biuro@kancelaria-kaczynska.pl
kancelaria-kaczynska.pl
tel: 608 537 489