POPOVICI NIȚU
STOICA & ASOCIAȚII
Attorneys at Law

239 Calea Dorobanți, 6th Executive Floor
Bucharest, 1st District, Postal Code 010567
Romania

Telephone: (0040) 21 317 79 19
Fax: (0040) 21 317 85 00 / 317 75 05

office@pnsa.ro
www.pnsa.ro

RO 15168518

DATA PRIVACY

OCTOBER 30, 2017

GDPR: Relations and responsibilities in the processing of personal data (controllers, processors and sub-processors)

There is no doubt that every company processes personal data (e.g. of its' employees', clients', contractual partners').

Most often, this also involves a constant barter between companies processing personal data and companies providing various services (e.g. HR, IT, payroll, datacenters, cloud services), both of them falling within the scope of the GDPR.

However, depending on whether a company processes personal data as a data controller or a data processor, the requirements and responsibilities under the GDPR may differ, and when a company is a data controller as well as a data processor, things might complicate.

So… is your company a data controller, a data processor or both?

The definitions of the data controller and the data processor remain the same under the GDPR, only their obligations and responsibilities are significantly amended:

- "controller" means 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;
- "processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Companies must screen each processing of personal data and ascertain the party responsible for determining the purposes and means of the processing. It may come as a result that for certain types of processing the company acts as a data controller, while for others the same company has a role as a data processor.

The next step will be to clearly understand and further implement the novelties brought by the GDPR regarding the relations between (a) controllers and controllers, (b)

controllers and processors and (c) processors and sub-processors.

a. Controller – Controller

Generally, data controllers act independent from one another. Yet sometimes two or more controllers jointly determine the purposes and means of processing and are considered, according to the GDPR, 'joint controllers'.

Consequently, they must conclude an agreement which shall stipulate, at least, the following:

- their respective responsibilities for compliance with the obligations under the GDPR;
- if considered necessary, designation of a contact point for data subjects;
- the roles and relations of the joint controllers vis-à-vis the data subjects.

However, irrespective of the terms of the arrangement:

- the data subjects may exercise his or her rights under the GDPR in respect of and against each of the controllers;
- controllers are jointly liable for the damage caused by processing which infringes the GDPR;
- a joint controller may be exempt from liability only if it proves that it is not in any way responsible for the damage;
- if a controller pays full compensation to data subjects, then it may claim back from the other controllers involved their part of the compensation.

b. Controller – Processor

The controller – processor relation was subject to many changes, the GDPR causing a shift in liabilities with regard to data processors.

The GDPR imposes direct legal compliance obligations on data processors, in addition to the obligations of the data controller. As a result, processors will be liable to data subjects for damages suffered as a result of non-compliance with the obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

Holding the data processor accountable under the GDPR puts even more pressure on the contract between the processor and the controller. For this reason, the GDPR requires that the activity of a processor shall be governed by a contract in writing (including in electronic form) that sets out (i) the subject-matter and duration of the processing, (ii) the nature and purpose of the processing, (iii) the type of personal data and categories of data subject and (iv) the obligations and rights of the controller. The contract shall stipulate, in particular, that the processor:

- processes the personal data only on documented instructions from the controller and informs the controller if it believes said instruction infringes the GDPR;

- ensures that persons authorised to process the personal data have committed themselves to confidentiality;
- takes all measures regarding the security of processing;
- assists the controller for the fulfilment of its obligations to respond to requests for exercising data subject's rights;
- upon request, deletes or returns all personal data to the controller at the end of the service contract;
- enables and contributes to compliance audits conducted by the controller or a representative of the controller.

In addition, the processor will have the following direct obligations:

- to keep records of the processing activities performed on behalf of the controller;
- to notify the controller without undue delay upon learning of data breaches;
- to take reasonable steps to secure data, such as encryption and pseudonymization, stability and disaster recovery, and regular security testing;
- to appoint a Data Protection Officer, if necessary;
- to cooperate with the Data Protection Authority.

From the controller's point of view, the GDPR imposes for the company to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of the GDPR and ensure the protection of the rights of the data subjects.

Taking into consideration that the controller remains liable for the damage caused by the processing, it must pay great attention when choosing the processor and concluding the contract.

c. Processors – sub-processors

In the course of business and, as a consequence, in the processing of personal data, more and more companies get involved. The processing chain is unlikely to stop with the processor, and therefore the GDPR contains provisions on the relation between the processor and the sub-processor.

Before engaging a sub-processor, the initial processor must have the prior specific or general written authorisation of the controller. In the case of a general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

Also, the same data protection obligations as set out in the contract between the data controller and the data processor (presented at point b) shall be imposed on the sub-processor by way of contract.

If the sub-processor fails to fulfil its data protection obligations, the initial processor will remain fully liable to the controller for the performance of the sub-processors obligations.

***

Last but not least, remember to choose wisely your processors and sub-processors and make sure the GDPR guides their activity and your relation!

This document is intended for informational purposes only, does not represent legal advice and does not focus on particular cases.

For further information or analysis on specific matters, please contact **Alexandru Ambrozie** (alexandru.ambrozie@pnsa.ro), **Luana Dragomirescu** (luana.dragomirescu@pnsa.ro) or **Ana Stoenescu** (ana.stoenescu@pnsa.ro).

For more information about Popovici Nițu Stoica & Asociații, please visit: www.pnsa.ro