POPOVICI NIȚU STOICA & ASOCIAȚII
Attorneys at Law

239 Calea Dorobanţi, 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

JANUARY 15, 2018

Data Privacy Impact Assessment at a glance / All you need to know

The EU General Data Protection Regulation (**GDPR**) requires all organizations to implement, before its entry into force on May 25th, 2018, a wide range of measures to protect the data assets and privacy of individuals and reduce the risk of breach by controllers or processors. These include accountability measures such as: running Data Privacy Impact Assessments, performing regular audits, reviews and updates of existing templates, supplier contracts and policies, activity records, internal training and awareness raising programs, and in certain cases appointing a Data Protection Officer.

Envisaged as a process for building and demonstrating compliance, the GDPR asks the companies to carry out **Data Privacy Impact Assessments (DPIA)**.

Scope of the DPIA

The DPIA is an instrument (a) for assessing the potential impact on privacy of the processes, information systems, software, devices or other initiatives which process personally identifiable information and (b) for designing the actions necessary in order to treat potential risks to the rights and freedoms of the individuals.

DPIA is an important tool for accountability, as it helps controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been designed and implemented in order to ensure compliance.

When does a DPIA become mandatory?

Not every processing operation requires carrying out a DPIA. DPIA becomes mandatory on any "likely to result high risks" processing activity.

A "likely to result high risks" processing activity will encompass activities such as:

- systematic and extensive evaluation of personal aspects, based on automated processing, including profiling, and on

which decisions concerning individuals are made;

- processing on a large scale of special categories of data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying individuals, data concerning health, data concerning sex life or sexual orientation, data relating to criminal convictions and offences;

- a systematic monitoring of a publicly accessible area on a large scale *(by reference to: the number of individuals concerned, the volume of data, the duration or permanence of the data processing activity or the geographical extent of the processing activity)*.

Other factors and criteria should be considered when assessing the high risk of a processing operation such as:

- matching or combining datasets (e.g. datasets originating from two or more data processing operations performed for different purposes and/or by different data controllers) in a way that would exceed the reasonable expectations of the individual;

- data concerning vulnerable individuals (e.g. children, persons requiring special protection such as mentally ill persons, asylum seekers, or the elderly, patients and, notably, employees in relations to their employees) and, generally, where an imbalance in the relationship between the position of the data subject and the controller can be identified;

- innovative use or applying new technological or organizational solutions (e.g. combining use of finger print and face recognition for improved physical access control);

- when the processing in itself "prevents data subjects from exercising a right or using a service or a contract". This includes processing operations that aims at allowing, modifying or refusing individuals' access to a service or entry into a contract.

Establishing the processing operations types triggering the obligation to carry out DPIA as well as any exceptions thereof shall ultimately fall with the Supervisory Authority of each member state. The Romanian Supervisory Authority has not published yet the list of such operations.

But generally, in cases where it is not clear whether a DPIA is required, it is recommended to carry out the DPIA nonetheless. With or without the obligation to carry out a DPIA, companies' general obligation to implement measures to appropriately manage the risks for the rights and freedoms of individuals remains.

Key points in carrying out a DPIA

Accountability. A DPIA may be carried out by companies internally or may be outsourced to either a third party or the data processor, acting for the data controller. But in all cases, the responsibility for ensuring that the DPIA is carried out remains with the data controller.

Structure. The controllers have flexibility to determine the precise structure and form of a DPIA.

Content. As a minimum, the DPIA must include: (a) the description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller, (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes, (c) an assessment of the risks to the rights and freedoms of individuals and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data, and to demonstrate compliance.

Consultation. When carrying out a DPIA, the views of data subjects or their representatives and the advice or the Data Privacy Officer (if already appointed) must be sought, but the controller is not obliged to implement them. For HR purposes, this is likely to be interpreted as an obligation to consult with works councils or trade unions.

Consulting the Supervisory Authority is required whenever residual risks are high and cannot be mitigated - such as where individuals may encounter significant or even irreversible consequences. In such case, the full DPIA must be communicated to the Supervisory Authority.

Disclosure. There is no obligation to publish or disclose the DPIA (unless specifically requested by the Supervisory Authority). However, publishing a summary or conclusions of the DPIA or even a statement that a DPIA has been conducted could foster trust in the controller's processing operations, demonstrating accountability and transparency; this is recommended especially in the educational and healthcare industries.

DPIA requirements for processing operations initiated before May 2018

As a general rule, a DPIA is only required for processing initiated after the coming into force of the GDPR on May 25th, 2018.

However, a DPIA should be carried out for existing processing if there is a change in the conditions of the processing (scope, purpose, personal data collected, identity of the data controllers or recipients, data retention period, technical and organizational measures etc.) or of the risks. Changes that lower the risk (based on a review of the risk analysis) will not trigger the requirement of the performance of a DPIA.

Consequences of non-compliance with DPIA requirements

Non-compliance with DPIA requirements can lead to fines imposed

by the Supervisory Authority. Failure to carry out the DPIA when the processing is subject to a DPIA, carrying out a DPIA in an incorrect way, or failing to consult the Supervisory Authority when	required, can result in an administrative fine of up to €10M or up to 2 % of the total worldwide annual turnover of the previous financial year, whichever is higher.

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) or **Luana Dragomirescu** (luana.dragomirescu@pnsa.ro).

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