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 29, 2018

ENFORCEMENT AND SANCTIONS UNDER THE GDPR

Maybe one of the most talked about part of the Regulation 679/2016 (GDPR), the significantly increased administrative fines are a central element in the new enforcement regime introduced by the Regulation.

Although the administrative fines will probably become the most powerful tool in the hands of the supervisory authorities for addressing non-compliance, they should be considered along with several other corrective measures, but also with the right to an effective judicial remedy of the individual against a controller.

We shall address below the most important aspects related to the right to a judicial remedy and compensation, as well as the corrective measures that may be imposed by the supervisory authority, with highlights on administrative fines and general criteria for establishing the amount of such fines.

Right to a Judicial Remedy and Right to Compensation

Each data subject has the right to an effective judicial remedy against:

- the supervisory authority, in case the supervisory authority does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged, as well as against a legally binding decision concerning the data subject;
- the controller or the processor, where he/she considers that his or her rights under the GDPR have been infringed as a result of the processing of his /her personal data.

An express right to compensation is granted to the data subject for any material or non-material damages suffered as a result of an infringement. There is no ceiling set to the right to compensation or to the size of liability, decisions that can be made against the controller, the processor or both.

The controllers should keep in mind that they are jointly liable with their processors and may be held liable for the entire damage, even if the fault belongs to the processor.

In order to mitigate this risk, the controllers should closely scrutinize the activity of their processors.

Proceedings against the controller and/or the processor may be brought before the courts where the data subject has his/her habitual residence or at the headquarters of the controller or processor.

Corrective Measures

Supervisory authorities will maintain prerogatives for monitoring and enforcing compliance with applicable data protection rules. These shall include possibility to carry out investigations, to notify the infringements and to obtain access to information, as well as to the premises of the controller or processor, including to the data processing equipment, and taking witness statements.

When talking about corrective powers of the supervisory authority, these shall include, notably, prerogatives such as: issuing warnings to controllers or processors whose intended processing operations are likely to infringe provisions of the GDPR; ordering the controller or processor to bring processing operations into compliance, but also more drastic measures such: imposing a temporary or definitive limitation including a ban on processing, ordering the suspension of data flows to a recipient in a third country or to an international organization, ordering the rectification or erasure of personal data or restriction of processing, withdrawing a certification or ordering the certification body to withdraw a certification and, at last but not least, issuing a reprimand (in case of minor infringements or if the fine likely to be imposed would constitute a disproportionate burden) and imposing administrative fines.

Administrative Fines

The administrative fine may be imposed either instead of or in addition to any of the above corrective measures, depending on the circumstances of each individual case, and in addition to the rights of data subjects to seek judicial remedy and compensations.

While the supervisory authority has discretionary powers on determining the level of the fine, the fine should be **dissuasive** (to send the message that infringements are not acceptable), **effective** (in stopping the infringement) and **proportionate** (to the size of the organization, as well as the size of the effects).

The criteria the supervisory authority is expected to use in the assessment both of whether a fine should be imposed and of the amount of the fine, are, among others:

- the nature, gravity, duration and consequences of the infringement;
- the negligent or intentional character of the infringement;
- the actions taken by the controller to prevent or mitigate the damage suffered by the data subjects;
- the degree of responsibility (such as the measures taken to ensure compliance with the obligations under the GDPR);
- any relevant previous infringements and compliance with previous measures ordered against the controller or processor;
- the manner in which the infringement became known to the

supervisory authority and degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects;
- the categories of personal data affected by the infringement (sensitive categories of data will bring greater fines and corrective measures than standard data);
- adherence to a code of conduct or approved certification (compliance with international security standards such as ISO 270001 may be considered to demonstrate that an organization is taking steps to implement appropriate measures under the GDPR), and
- any other aggravating or mitigating factor, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

You may be noticing that there is a particular focus on organizational culture towards data protection and being able to demonstrate compliance is almost as important as being compliant.

In light of this, all organizations need to be thinking about the extent to which they are taking appropriate steps, sufficiently far in advance, to meet their obligations under the GDPR. You do not want to find yourself having to explain, while having had a breach, why you had not yet started on the road to the GDPR compliance, as this may be clear evidence of negligence.

If talking practical examples, one of the highest fines in EU was imposed in connection with a stolen customer database, where the data was allegedly accessed during an attack on three vulnerable webpages. Poor management, failure to investigate and ensure that the most basic security measures were in place, as well as the failure to prevent attacks on a smaller scale on previous occasions (as part of the steps that the organization ought to have taken if it was seeking to be responsible in dealing with personal data) were considered aggravating factors retained by the supervisory authority.

The GDPR identifies a wide range of breaches, including purely procedural infringements, to which the administrative fines shall be applied. There are two tiers of administrative fines.

The lower tier of fines, which are **up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher**, apply in case of:

- failure to obtain parental consent in case of services offered to a child;
- failure to comply with privacy by design and privacy by default principles;
- in case of joint controllers, failure to agree to their respective compliance obligations;
- failure to designate a representative in the EU for controllers or processors established outside EU;
- failure to comply with requirements for appointing and acting as data processor;
- failure to maintain adequate records of processing activities;
- failure to cooperate with the supervisory authority;

- failure to implement appropriate organizational and technical security measures;
- failure to notify data breaches;
- failure to carry out a data privacy impact assessment (or improperly carry out such assessment) or consult the supervisory authority when a processing would result in a high risk;
- failure to appoint a data privacy officer;
- infringement of the provisions of the code of conduct or failure to comply with certification requirements (where appropriate).

The second/higher tier of fines **up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher**, will be imposed for breaches of any of the principles going straight to the heart of the GDPR:

- infringement of the basic principles for data processing: lawfully, fairly and in a transparent manner, collected for specified, explicit and legitimate purposes, adequate, relevant and limited to what is necessary, accurate and, where necessary, kept up to date, retained only for as long as necessary and processed in an appropriate manner to maintain security (including sensitive data and conditions for consent);
- failure to comply with the data subjects' rights;
- failure to comply with the requirements for the transfer of data outside EEA;
- failure to comply with any national obligation;
- failure to comply with an order issued by the supervisory authority;
- failure to provide access to a supervisory authority.

Infringement of GDPR different provisions may lead, among others, to an administrative fine that may not exceed the amount specified for the most serious of the infringements.

Set aside, a single breach of GDPR can lead to multiple consequences for controllers and processors so the best answer is to make sure that you are not negligent, to make sure you have taken steps to mitigate damage suffered by data subjects, to take into account appropriate technical and organizational measures and to effectively deal with the GDPR.

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