November 2017

NEW DATA PROTECTION GUIDELINES ON GDPR

Important news in the data privacy field after the Article 29 Working Party Plenary held in October 2017: the drafts of two new guidelines were finalized and a final form of a third one was adopted. The guidelines are aimed at ensuring a harmonized application of the GDPR, after 25 May 2018.

Article 29 Working Party adopted in October the final version of the *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.* The above Guidelines analyze and interpret the provisions of art. 35 of the GDPR, which raised numerous discussions and concerns amongst interested entities, particularly given the novel character of the DPIA obligation and the uncertainty on its practical approach.

Thus, the Guidelines offer important indications and clarifications on matters such as: (i) the DPIA obligations of data controllers; (ii) how such data controllers establish if the personal data protection operations they perform are "*likely to result in a high risk to the rights and freedoms of natural persons*"[1] or not; (iii) when should a PIA be performed; (iv) the methodology for carrying out the DPIA, etc.

Another two guidelines were finalized in the October Plenary of the Article 29 Working Party, namely the "*Guidelines on Personal data breach notification under Regulation 2016/679*" ("**Data breach notification Guidelines**") and the "*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*" ("**Automated individual decision-making and Profiling Guidelines**").

The Data breach notification Guidelines are based on art. 33 GDPR and regulate the obligations of the responsible entities in case of a data breach - "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.*"[2]

The Guidelines provide a comprehensive description of the meaning of "data breach", applicable procedures and communication requirements related thereto, and analyzes certain aspects such as: (i) types of data breaches; (ii) the data processor's obligations in case of a data breach; (iii) conditions when notifications are not required; (iv) communication to the data subjects; and (v) the role of the data protection officer. Moreover, the Guidelines provide a flowchart presenting data breach notification requirements and practical examples of personal data breaches, for a better understanding of these requirements.

The other Guidelines finalized but not yet adopted by the Article 29 Working Party refer to the processing of personal data within certain processes that are recently more widely

[1] Art. 35 paragraph 1, GDPR

[2] Art. 4 paragraph 12, GDPR

used, primarily due to significant technology progresses--namely the automated decision-making and profiling purposes.

Profiling means "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements*."[3]

As regards the automated decision-making processes, their main characteristic consists of "*the ability they offer to make decisions by technological means without human involvement*".[4]

According to the Automated individual decision-making and Profiling Guidelines and art. 22 of the GDPR[5], the general rule is that such activities (if based solely on automated processing) are prohibited, unless certain exceptions apply.

The Guidelines also provide an overview of the provisions applicable to profiling and automated decision-making, such as: (i) data protection principles to be observed (e.g. data minimization, accuracy, purpose limitation, etc.); (ii) lawful bases for processing (e.g. legitimate interest, compliance with a legal obligation, performance of a contract, etc.); or (iii) the data subjects' rights (e.g. right to be informed, right to object, right of access, etc.)

These last two Guidelines are subject to public debate. Proposals on their content may be formulated by 28 November 2017.

For details on the above, you may consult the full content of the Guidelines at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[3] Art. 4 paragraph 4, GDPR

[4] Article 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, page 7

[5] Art. 22 paragraphs 1 and 2 GDPR: "(1) *The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*

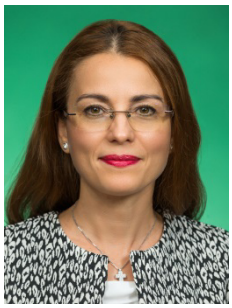
(2) Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent."

About WOLF THEISS

Wolf Theiss is one of the leading law firms in Central, Eastern and Southeastern Europe (CEE/SEE). We have built our reputation on a combination of unrivalled local knowledge and strong international capability. We opened our first office in Vienna almost 60 years ago. Our team now brings together over 340 lawyers from a diverse range of backgrounds, working in offices in 13 countries throughout the CEE/SEE region.

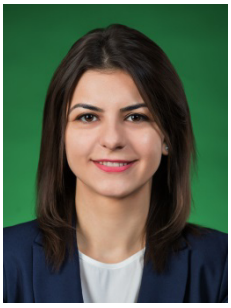
Our dedicated Wolf Theiss Cross-Border Data Privacy Task Force is comprised of experienced legal and IT professionals who have specific experience in providing integrated solutions to our clients in swiftly developing areas of law such as GDPR, Anti-Money Laundering, compliance, data and cyber security. We work across all industry and business sectors that are impacted by the tremendous changes and challenges that have been introduced by the technological innovations of the digital age.

For more information about our services, please contact:



Maria Maxim
Partner
maria.maxim@wolftheiss.com
T: +40 21 308 8100

Roland Marko
Partner
roland.marko@wolftheiss.com
T: +43 1 51510 1880



Daniela Dosan
Associate
daniela.dosan@wolftheiss.com
T: +40 21 308 8100