

A NEW DECISION ADOPTED BY THE DATA PROTECTION AUTHORITY IN THE IMPLEMENTATION OF THE GDPR IN ROMANIA

A new decision of the Romanian Data Protection Authority (the "**Authority**") entered into force on 23 October 2018 as a new instrument in the implementation of the Regulation (EU) no. 2016/679 on the protection of natural persons regarding the processing of personal data and on the free movement of such data (the "**GDPR**") in Romania.

Decision no. 161/2018 ("**Decision no. 161/2018**") provides the legal framework on investigations carried out by the Authority.

PROCEDURAL RULES FOR CONDUCTING INVESTIGATIONS

General provisions

Decision no. 161/2018 mainly integrates the previous rules on conducting investigations, while further developing in particular on field investigations. The Data Protection Authority may initiate investigations *ex officio* or following a complaint.

Investigations may be carried out: (i) on the field, either as dawn raids or announced, (ii) in writing or (iii) at the Authority's seat. *Ex officio* investigations may also take the form of data protection audits. Decision 161/2018 does not elaborate on what an audit means and what would be the result of such an investigation; however, we expect this would be an extensive investigation that may result in a remedy plan imposed by the Authority to the entity under control, without excluding also the possibility of the Authority to impose fines for identified breaches.

During an investigation the Authority is entitled to verify any matter related to the processing of personal data, as well as any equipment or means under in data processing. An investigation may be suspended or postponed, for justified reasons, including upon request of the entity under control.

Sanctions of up to EUR 300,000 may be imposed by the investigation team upon finalizing the investigation. Any sanction exceeding EUR 300,000 may only be ordered by the President of the Authority.

Key issues

- Decision 161/2018 mainly takes over the rules already applicable to carrying out investigations by the Data Protection Authority.
- The investigation powers of the Authority are extended in case of dawn raids and the Authority is granted the power to also conduct investigations at its office and in exceptional cases to apply sanctions without even summoning the entity under control.
- The investigation team may check any matters related to data processing and may access all documents, equipment or storage means, while being entitled to use any audio/video recording or storage means it deems necessary for the investigation.
- Investigations are always carried out in the presence of a representative of the entity under control, who needs to ensure the availability of a relevant person as to avoid delaying the investigation.

The investigation team may also impose corrective measures such as observing requests from data subjects, ensuring compliance of data processing operations, informing data subjects on breaches. More severe measures such as temporary or definitive limitation of data processing, restriction or interdiction of data processing, withdrawal of certifications may only be imposed by the President of the Authority.

After the expiry of the term set for fulfilling the measures imposed by the Authority, a new investigation may be initiated if the investigated entity fails to provide the Authority with proof of compliance.

The sanctioning minutes issued by the Authority may be challenged within 15 days as of the date of communication.

Dawn raids

Dawn raids may be carried out at any location where the controlled entity operates or where personal data is processed. The Authority may retain documents in certified copy and may put under seal any documents, equipment or storage means, while it may also use any audio-video or photo recording, or storage means it deems necessary for the investigation.

The inspection staff is bound by professional secrecy regarding confidential or classified information obtained during the investigation. Companies will need to be careful in ensuring proper procedures for establishing and dealing with confidential or classified information in relation to data processing operations.

Before starting the investigation, the investigators have an obligation to present their control badge and an empowerment issued by the president of the Data Protection Authority.

Any investigation may be carried out between 8 AM and 6 PM and in the presence of a representative of the entity under control. The entity under control may not delay the investigation by not ensuring the presence of a representative. Any delay may be considered a hindrance to the investigation.

The controlled entity may not oppose confidentiality when required to present any document, information or clarifications and must not delay the investigation in any way. The control team may interrogate any persons they may deem relevant and necessary for the investigation.

In case the control body is prevented in any manner from conducting the investigation, the Data Protection Authority may obtain a judicial authorisation, issued by the president of the Bucharest Court of Appeal. The entity under control may be obliged to pay RON 3,000 (approx. EUR 643) fine for each day of delay in the investigation.

When the Authority requests the authorization of the court, the court decision is communicated also to the entity under investigation and it specifies all locations where the investigation will take place. The judicial decision may be challenged with the Supreme Court within 72 hours as of communication. Such remedy does not suspend the performance of the investigation.

Key issues

- The entity under control should take all measures not to delay or hinder the investigation in any manner, subject to potential fines of Ron 3,000 (approx. EUR 643) per each day of delay.
- The Authority may request assistance from the police during the investigation or even prior to it if there are any indications of an opposition from the entity under control.
- Investigations on public institutions and authorities result in milder consequences and a predetermined warning sanction.

Investigations at the Data Protection Authority's seat

The Authority may summon any entity involved in data processing operations at its office, requesting that the latter brings relevant documents, recordings or IT equipment. In exceptional cases, when the Authority decides it already has all relevant proof, it may issue a sanctioning decision without even summoning the entity under control.

The entity under control may submit observations to the sanctioning minutes within 15 days as of communication.

Investigations conducted in writing

The Data Protection Authority may also conduct investigations solely in writing. In this scenario, the Authority notifies the relevant entity of the investigation and requests documents, information and relevant data. The entity under investigation is obliged to provide the Authority with the requested documents and information, in certified copy. After analysing such documents and information, the Authority may decide to initiate a field investigation or an investigation at its seat, to issue a sanctioning minute or it may close the investigation.

The entity under control may submit observations to the sanctioning minutes within 15 days as of communication.

Investigations conducted on public institutions or authorities

Investigations conducted on public institutions and authorities may result in milder consequences for the entity under control. If breaches are identified during the investigation, the investigation team will apply a predetermined warning sanction and will prepare a remedy plan for the respective public body to implement.

The calendar for implementing the remedy plan is set by the Authority depending on the risks related to the breaches, as well as on the actions that need to be taken to complete the remedy plan. If the Authority ascertains that the remedy plan was not fulfilled within 10 days as of the expiry of the set term, it may start a new investigation.

SANCTIONS

Decision no. 161/2018 also enters details on how sanctions regulated by the GDPR apply. The Authority may impose fines or certain corrective measures on the companies and may also give warnings.

Fines over EUR 300,000 may only be imposed by the president of the Data Protection Authority. Decision no. 161/2018 also sets a RON 3,000 (approx. EUR 643) per day penalty for each day of delay in complying with the corrective measures or for failing to provide the requested documents.

Certain corrective measures may only be imposed by the President of the Authority. In case the controlled entity does not comply with any corrective measures imposed to it, a new investigation may be performed.

Any sanctioning minutes may be challenged within 15 days as of communication. The challenge will only suspend the obligation to pay the fine and not other measures imposed by the Authority.

CONTACTS



Nadia Badea
Partner

T +40 21 6666 102
E nadia.badea
@cliffordchance.com



Ecaterina Burlacu
Senior Associate

T +40 21 6666 144
M +40 741 041 605
E ecaterina.burlacu
@cliffordchance.com

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance Badea SPRL, Excelsior Center, 28-30 Academiei Street, 12th Floor, Sector 1, Bucharest, 010016, Romania

© Clifford Chance 2018

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Doha • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.