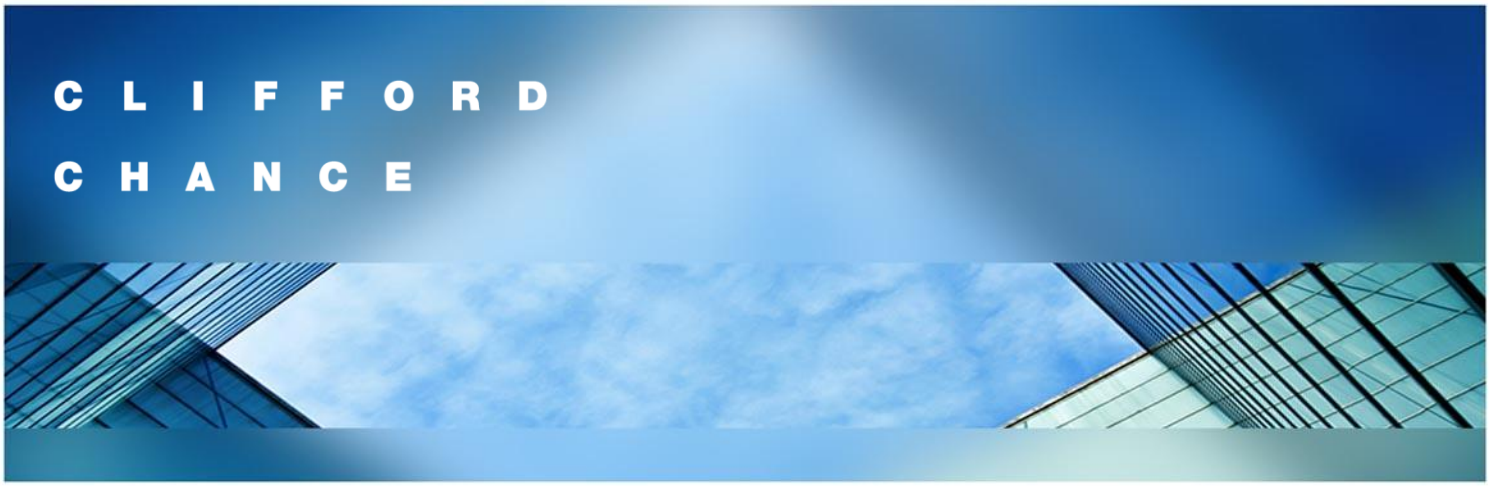

THE CNPD PUBLISHES 18 DECISIONS AND IMPOSES SANCTIONS UNDER THE GDPR.

On 7 June 2021, the Luxembourg data protection authority (the "**CNPD**") published 18 decisions based on investigations carried out in 2019.[1] These long-awaited decisions are the first the CNPD published since the entry into application of the EU General Data Protection Regulation ("**GDPR**") and highlight certain expectations from the CNPD in relation to GDPR compliance.

CONTEXT

Pursuant to the GDPR and the Luxembourg Law of 1 August 2018 (the "**2018 Law**"), the CNPD has the mission to monitor and enforce the application of the GDPR in Luxembourg. To that end, the CNPD is empowered to carry out investigations, including in the form of audits and on-site inspections ("**OSI**").

The CNPD focuses its monitoring and enforcement efforts on selected subject matters. As highlighted in the 2018 and 2019 annual reports, in 2019, the CNPD carried out 25 thematic investigations on data protection officers ("**DPO**") along with 33 OSIs (against 12 in 2018) on video surveillance, geolocation and marketing practices across both the public and the private sectors. These decisions relate to the same topics: **12 relate to the DPO, 4 to video surveillance and 2 to geolocation.**

The decisions notably showcase sanctions: **6 administrative fines (ranging from EUR 1.000 to 18.000) and 3 reprimands, as well as 9 closing decisions for lack of breach.** The decisions of the CNPD indeed document the outcome given to the above inspections by the CNPD restricted panel (*formation restreinte*), taking into account both the proposal by the designated chief investigator (*chef d'enquête*) and the responses by the audited entity.

KEY HIGHLIGHTS FROM THE DECISIONS

It shall be noted that, across all decisions, the CNPD assesses compliance at the date of the OSI. However, mitigation measures taken by entities during or after the investigation are taken into account. The CNPD further considers that, in case of joint-controllership, the investigation does not need to be carried out in relation to all joint-controllers.

Key issues

- The CNPD published 18 decisions based on investigations carried out in 2019.
- The CNPD imposed fines ranging from EUR 1.000 to 18.000.
- The decisions are based on available guidance issued by the CNPD itself and the EDPB, as well as what the *chef d'enquête* considers to be good practice.
- Compliance is assessed at the date of the investigation.
- The decisions from the CNPD may be challenged following on the basis of the rules of Luxembourg administrative procedure.
- In 2021 the CNPD will conduct thematic investigations concerning records of processing activities and international data transfers.

[1] The 18 decisions may be found here : https://cnpd.public.lu/en/actualites/national/2021/06/premieres-decisions.html

We have selected below key highlights from the decisions.

Expectations from Data Protection Officers

Pursuant to the GDPR, entities must ensure that their DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. In a decision, the CNPD found that, although a DPO at group-level had been designated, it was not directly involved in issues of the Luxembourg entity and did not have sufficient resources (i.e., at Luxembourg level, the point of contact for the DPO was the sole internal legal counsel and the DPO was not part of the GDPR committee). The CNPD further found that the required time and resources made available to the DPO where not sufficiently documented.

According to available guidance, the DPO must be independent. It may fulfil other tasks and duties provided they do not result in a conflict of interest. The CNPD considers that **there is a conflict of interest where a "*Chief Compliance Officer*" is also the designated DPO**, due to the DPO being responsible in the design of AML/KYC processing activities in its role of compliance officer.

The DPO must, pursuant to the GDPR, be designated based on its expert knowledge of data protection law and practices in order to fulfil its tasks. The CNPD considered, in respect of an entity of the insurance sector, that the DPO should have had **at least 3 years of professional experience** (irrespective of the trainings followed by said DPO at the time of the OSI).

Transparency regarding video surveillance

Pursuant to the data minimisation principle and as further elaborated in the CNPD's guidelines on video-surveillance,[2] cameras which film places reserved for employees at the workplace for private use (e.g., a cafeteria) are in principle considered disproportionate. In a decision, the CNPD found that cameras which were installed in a manner that also views the terrace of the canteen unintentionally, were not aligned with the data minimisation principle.

Data subjects (i.e., the employees in this case) must be informed of the processing of personal data via the video-surveillance system. In another decision, the CNPD noted that **informing the staff delegation does not equate to informing the employees**, and that a sign warning employees of the video surveillance, does not contain the required information pursuant to art. 12 to 14 of the GDPR.

A third decision concerns cameras directed outside of an entity's premises and which included surrounding areas in their field of view. The entity was pursuing a layered approach to information with a first sign containing the essential information of the processing, containing a reference where to find a second notice with more complete information (which is recommender under available guidance on transparency). The CNPD however found that simply displaying the old vignette delivered by the CNPD under the pre-GDPR regime and warning third parties of the presence of cameras was insufficient, even as a first layer. The CNPD also noticed that third parties who did not work within the premises did not have access to the privacy policy (which was only

[2] Available at : https://cnpd.public.lu/content/dam/cnpd/fr/dossiers-thematiques/videosurveillance/CNPD-Lignes-directrices-videosurveillance.pdf

communicated to the employees) containing the additional information on the processing.

Retention and transparency on location data

According to the principle of data minimisation, and as further specified in the CNPD's guidelines on the geolocation of employee vehicles,[3] the CNPD set out specific retention periods for the personal data processed in this context. In a decision, the CNPD found that the entity did not align its retention periods with the above guidelines and retained personal data for longer than necessary.

In this decision, the CNPD also found that the entity did not document the information to their employees – a simple declaration by the staff delegation that employees were informed of the existence of the geolocation was not sufficient evidence according to the CNPD.

In a second decision regarding the geolocation related processing by a communal administration (*commune*), the CNPD found that, although information to the data subjects may be provided orally, evidence of such information must in any case be documented (i.e., in writing).

LESSONS TO BE LEARNED

With these 18 decisions, the CNPD clearly shows that OSI are being conducted and that it is willing to impose fines if necessary. We however note that, so far, the financial sector does not seem to be the focus of the CNPD.

It is interesting to note that the decisions are based on available guidance issued by the CNPD itself and the EDPB, as well as what the *chef d'enquête* considers to be good practice. Entities must therefore ensure that all processes and procedures are in place and that their compliance with the GDPR is adequately documented.

Decisions of the CNPD may be contested according to the rules of Luxembourg administrative procedure. Entities have 3 months from the notification of the decision to challenge it (via a *recours en reformation*) before the administrative tribunal.

Going forward, in 2021, the CNPD will conduct thematic investigations concerning records of processing activities (compliance with article 30 of the GDPR) and international data transfers (notably following the *Schrems II* ruling of the European Court of Justice).

[3] Available at : https://cnpd.public.lu/content/dam/cnpd/fr/dossiers-thematiques/geolocalisation/Lignes-directrices-geolocalisation-vehicules.pdf

CONTACTS

Charles-Henri Laevens
Senior Associate

T +35 485050 485
E charleshenri.laevens@cliffordchance.com

Ottavio Covolo
Associate

T +35 485050 221
E Ottavio.covolo@cliffordchance.com