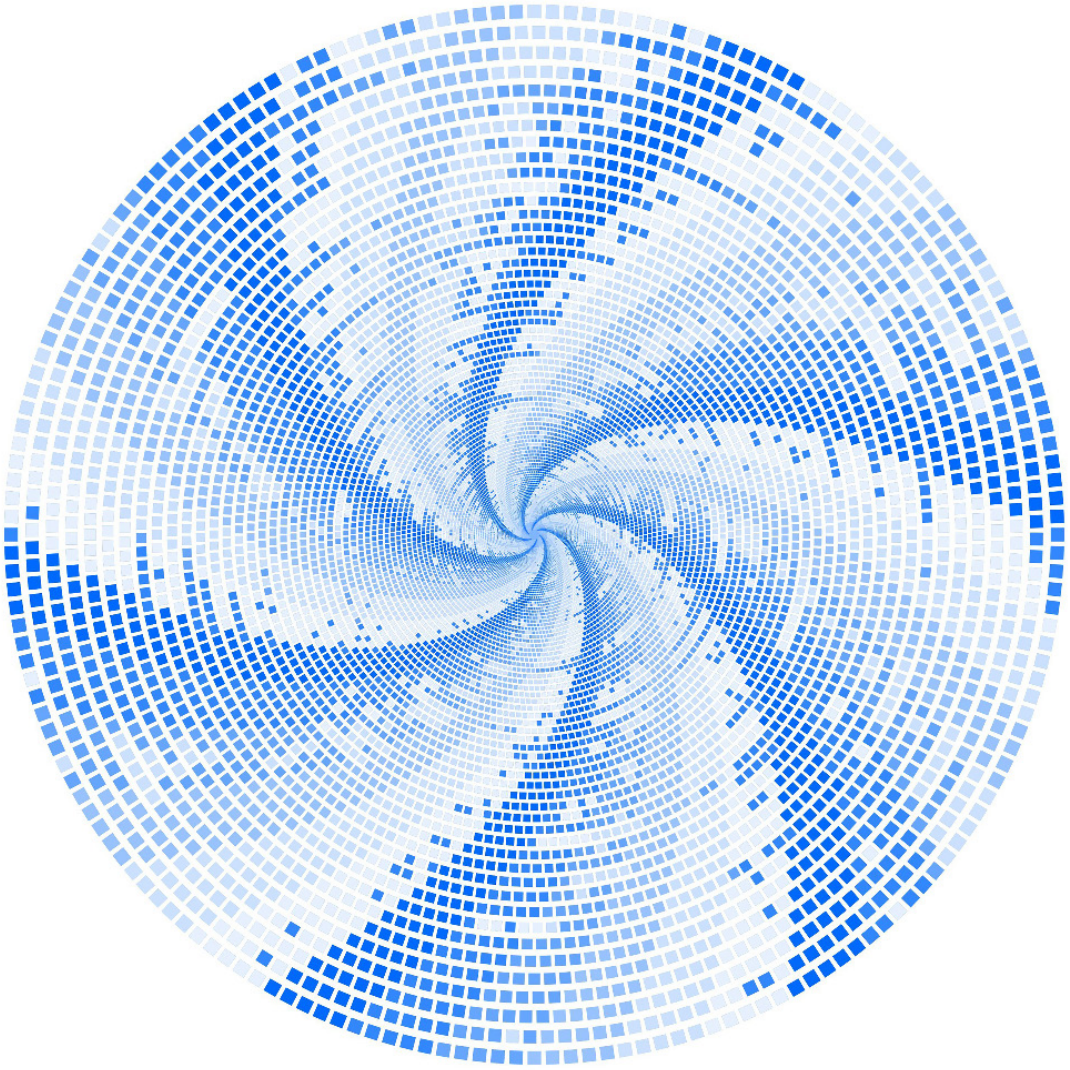
Deloitte.



Deloitte view on Belgian DPA Decision

Introduction

On April 28, 2020, the Litigation Chamber of the Belgian Data Protection Authority ("DPA or Authority")[1] imposed a fine of €50.000 on a company for non-compliance with the requirements under the General Data Protection Regulation ("GDPR")[2] related to the independent role of the data protection officer ("DPO").

On the one hand, the decision[3] clarified interesting aspects with regard to the DPO function and the expectations attached to it; on the other hand, it further shed light on a number of elements related to accountability, the data breach notification procedure, as well as a few procedural aspects including the duty of organisations to co-operate with the Authority during the inspection procedure. These important points were unfortunately missed from many of the analyses that followed the publication of this decision, focusing solely on the DPO role and, in particular, its incompatibility with other roles.

[1] https://www.gegevensbeschermingsautoriteit.be/

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[3] https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Beslissing_GK_18-2020_NL_.pdf; https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Beslissing_GK_18-2020_FR_.pdf.

Highlights of this Decision

Procedural aspects & collaboration with the DPA

By replying to the defendant's allegations that the case suffered procedural flaws, mainly because the inspection had largely been carried out by a service that acted outside of its competence[4], the DPA affirmed the single and unified nature of the investigative process.

To the eyes of the Litigation Chamber what counts is to ensure that the case is treated in a fair and objective manner throughout the entire process flow. Thus, the decision seems to have implicitly ruled out the view that a strict "compartmentalization" of roles exist between the different DPA services involved in the investigation. Instead of narrowly responding to the defendant's claim as to whether the service that is, according to the law, competent to undertake the inspection did it effectively, the Authority looked into whether the entire process had secured for the defendant the opportunity to move forward its argumentation and if the entire process respected its right to defence.

In its reasoning, the Litigation Chamber appears to accept in general that the DPA services that *de facto* have to be involved at an earlier stage of the investigation before the Inspection Service takes over, have the obligation to detect any *serious indications* of a data protection infringement[5]. This is a task that, in our view, practically requires the collection firstly, and the assessment later, of (the pertinence) of certain evidence albeit this evidence has been collected during the initial phases of the investigation process.

Accordingly, the DPA clarified in this decision that what practically counts during the investigation process is to ensure that the most fundamental procedural guarantee, being the *defendant's* right *to contradict the allegations expressed against it*, is effectively respected. In the case at hand, the Litigation Chamber found that this had fully been adhered to, during the process.

With regard to the duty of co-operation, the argumentation of the Litigation Chamber seems to suggest that it expects sufficiently *detailed and comprehensive* answers to the queries it addresses to organisations during the investigation process. Accordingly, although the DPA inferred that the exchange of letters with the justification needed was the standard way for proceeding with the DPA's enquiries, it also left the door open to additional avenues that the defendant could suggest in order to progress on the investigation. In this case, for example, the decision regarded positively the fact that the defendant proposed a consultation with the DPA, in order to clarify the methodology followed in the risk analysis of personal data breaches points of the evidence (see below).

Another interesting informative point of the decision is the approach of the DPA to common behavioral means that, usually, defendants adopt in order to blur the co-operation process or turn arguments to their favor during an investigation. These means are commonly known as the "Ten D's" in the language of the public policy advocacy. They include, indicatively, the attempts to shift the point of attention to non-substantial elements of the file other than those brought up by the counter-party (inflection), or to delay to provide the requested explanations or to deny admitting objective and true elements of the file[6]. In the case at hand the Chamber of Litigation did not need to take any decision on whether or not the defendant had indeed employed any of the "Ten D's" techniques. However, it is interesting to see that the usage of some of those techniques by the defendant was put forward in the Inspection report as obstacles to the duty to cooperate. The Inspection's arguments, although not followed by the Litigation Chamber, practically show that those methods currently represent negatively-perceived "defence" practices in general. Further, this decision shows that such techniques can potentially be considered by the DPA as a deterrent to a fruitful investigation.

The Litigation Chamber motivated that the grounds raised by the Inspection Service did not suffice to establish a factual violation of the defendant's obligation to co-operate. According to its reasoning, it was clear that, based on the factual observations outlined above (substantiated correspondence and defendant's readiness to consult with the DPA), the defendant fulfilled adequately its co-operation duty and, hence, there was no violation of Article 31 GDPR[7].

[4] According to the defendant, the DPA's Front Office has surpassed its scope of competence during the investigation phase while the Inspection Service, though competent to initiate the inspection by law, did not proceed to investigation.

[5] According to the decision, the Executive Committee did fulfil its role in this respect, as per art. 63, 1° of the Act of 3 December 2017 (rev.) establishing the Data Protection Authority – provision quoted in the decision.

[6] Explanations on the "Ten D's" concept can be found at: http://www.aalep.eu/recognizing-your-opposition-tactics-and-responding-them (hyperlink quoted in the DPA decision).

[7] This article stipulates the duty of co-operation of any organisation, be it a controller or processor, with the controlling authority, upon its request, in the performance of its tasks.

Highlights of this Decision (continued)

Accountability principle in the context of data breaches

According to the report of the Inspection Service, the risk analysis related to the notification of data breaches, which was performed by a team of company's business representatives, systematically indicated a low or insignificantly low risk in the assessments performed during the previous year. Moreover, according to the Inspection, the defendant failed to provide a clear reasoning about how the company arrived at these results concretely and this despite the questions asked by the DPA on this point.

The Inspection Report had also underlined as the defendant's failure the fact that, according to the risk evaluation process followed by the defendant and which was described in a RACI matrix, the DPO was *generally not consulted, but only informed* of the assessment results once the analysis was completed.

On this point, the defendant purported that there was no legal obligation for the DPA to verify in detail the risk evaluation process of an organisation. It further claimed that it had sufficiently clarified the methodology it had put in place to perform the risk analysis related to the notification of data breaches. The defendant also added that, on top of its explanations by letter, it had offered to provide more clarifications on the reasoning it had followed to evaluate the relevant risks during a (subsequent) consultation with the Authority. The Litigation Chamber accepted that the defendant had sufficiently responded to the questions of the Inspection Service through the evidence it furnished and, therefore, pronounced that there had been no violation of Articles 5.2, 24.1 and 33 of the GDPR.

Although the Litigation Chamber decided in favor of the defendant with regard to the evaluation of risks during the data breach notification process it has set up, it put forward some key practical points related to how accountability ties up to the data controllers' obligations including on data breaches.

We strongly recommend any company to reflect on these key points, check to what extent they could be relevant to them and take appropriate action accordingly:

01. There is a general obligation of each data controller to document any type of breach insofar as it affects personal data, be it of a high or minimal risk. This in a transparent manner, in order, to be able to furnish sufficient evidence to the DPA whenever asked.
02. Any document describing the data breach notification process, be it a RACI matrix, a policy or an operating procedure, must demonstrate that the DPO is effectively involved in the process and exercises the consultative role he/she has to ensure, according to the GDPR. The reasoning of the decision, as well as of the Inspection Report, clearly shows that any such diagram or procedure may become a piece of evidence subject to the Authority's assessment during an investigation.
03. Accountability is an overarching principle that transverses all obligations stipulated in the GDPR. It clearly surpasses the boundaries of Article 5.1, being the one laying down the foundational principles of personal data protection. According to the Litigation Chamber, the accountability principle clearly extends further down to the entire GDPR text, to cover for example data controllers' Article 33 obligations related to the notification of personal data breaches.

Highlights of this Decision (continued)

Accountability principle in the context of data breaches

04. To illustrate how the accountability objective also applies to the (personal) data breach notification obligations, the decision quoted specific extracts of the guideline adopted by the Article 29 Data Protection Working Party (WP) on this topic[8]. The decision precisely adhered to the WP's position, that is, that the obligation to keep internal documentation on any personal data breach derives from the accountability principle articulated in art. 5.2 GDPR. It then linked its reasoning to another citation of this guideline, stating that while the data controller is free to choose in which structure it would document a breach, it should however not miss to include certain mandatory elements in it (being the ones set out in art. 33 of the GDPR)[9]. The decision also aligned explicitly to another citation of the guideline, referring to the data controller's obligation to keep this information as the controlling authority could ask to check it as proof of the data controller's compliance with the obligations stipulated in art. 33 or, more generally, with the accountability principle. Finally, the Litigation Chamber had subscribed explicitly to the practical effect of non-compliance as it is stated on the WP's guideline: that any failure to correctly document a breach could give rise to the controlling authority's investigative and corrective powers and/or its competence to impose an administrative fine[10].
05. The Litigation Chamber seemed to appreciate the fact that the defendant had put in place a tool to enable its staff to report possible data breaches, as well as the necessary policies and training(s) to enhance staff awareness of data incidents.

Based on the above key elements of the decision, it is clear to us, that the accountability point strongly emphasised by the Litigation Chamber - albeit already in the WP29 guidelines - is becoming a significant matter of attention for regulatory enforcement. In summary, controllers need to document all personal data breaches, regardless of the level of risk they entail, in accordance with GDPR Art 33(5), enabling verification of compliance by the supervisory authority. This means that, in a proper accountability framework, every controller should create a methodology and implement all appropriate measures to document all reportable and non-reportable breaches, facts, consequences and corrective actions in a way that is transparent to the supervisory authorities. Failure to properly document a breach could lead to the authority exercising its powers, including imposing sanctions.

[8] WP 250.Rev01, Guidelines on personal data breach notification, adopted on 3 October 2017 and as revised and adopted on 6 February 2018 by the EDPB, p. 26 and ff.

[9] These elements are in summary: the information concerning the breach, including its cause(s); the related facts and types of personal data affected; the results and consequences of the breach, as well as the measures taken by the data controller to mitigate its effects.

[10] Deriving from art. 58 and 83 GDPR respectively.

The Role of the DPO

Involvement of the DPO in issues which relate to the protection of personal data

As mentioned above, the DPA further questioned the level of involvement of the DPO in the discussions related to the evaluation of data breaches. According to the defendant, it was sufficient that their data breach procedure was keeping the DPO informed and that this step of the process was in line with the GDPR prerogative to *involve the DPO in a timely and appropriate manner in all issues related to the protection of personal data*[11]. On the contrary, the Litigation Chamber clearly contested this interpretation, stating that *"The position of the defendant is not in accordance with the ratio legis [of the GDPR] and is not a meaningful interpretation of article 38.1 GDPR. By reducing the involvement of the Data Protection Officer to merely (retrospectively) informing him of a decision, his function is eroded."*[12]

As in the accountability case, the Litigation Chamber supported its position by referring to another guideline of the WP29, the one relevant to the position of the DPO[13]. Accordingly, it emphasized the EU regulators' recommendation to involve the DPO as early as possible in all data protection related matters. It further stressed how important it was to ensure that the DPO was consulted and actively involved in the discussions from the outset, rather than simply be informed of the outcome of the risk assessment. For the Litigation Chamber, the effective involvement of the DPO as from an early phase of the evaluation process represents a principle of "good governance" in any organisation and, hence, considered to be fully aligned with "the privacy by design" principle.

It is therefore of fundamental value to properly and clearly reflect the DPO's involvement in the data breach policies and procedures but also in the reality of the DPO's day-to-day relations with the company's management and staff, through appropriate training and by fostering a culture of compliance.

CCO/DPO conflict of interest

This part of the decision has raised a few eyebrows because, in our view, the DPA's reasoning was placed and interpreted outside of the context and facts of the specific case. In this specific situation, it appears that the individual who was effectively fulfilling the DPO role also held cumulatively the positions of head of Compliance, Risk Management and Internal Audit.

The Belgian DPA concluded that the defendant violated article 38.6 GDPR because of a conflict of interest with the other functions that the specific individual designated as DPO had to fulfill at the same time. According to the arguments of the Litigation Chamber, the defendant failed to prove that the tasks pertaining to his other positions were not incompatible with the DPO role he assumed in parallel.

It is important to acknowledge the nuance of the reasoning followed by the DPA on this point. While the DPA acknowledged the generally-common practice of having a DPO engaged or involved in other functions that would not compromise his ability to advise independently[14], it took a strict stand in this case, confirming the incompatibility of the DPO function with the simultaneous occupation of 3 (three) other managerial roles which, by definition, entail a decision-making power.

[11] Art. 38.1 GDPR; notably, the defendant argued that no specific obligation to consult with the DPO derives from this article.

[12] Free translation from the original Dutch text into English.

[13] WP243 rev.01, Guidelines on Data Protection Officers (DPOs) adopted on 13 December 2016 and as last revised and adopted on 5 April 2017.

[14] On this point, the Litigation Chamber subscribes to the letter of art. 38.6 GDPR and the interpretation given by WP29 guidelines (see footnote above); hence, it confirmed that the DPO may have other functions and be entrusted with other tasks and duties to the extent that the latter do not give rise to any conflicts of interest.

The Role of the DPO (continued)

CCO/DPO conflict of interest

According to the DPA's reasoning on this point, having the same person in these key management positions would practically mean that the DPO has "inherited" by definition operational responsibilities. These, in turn, would unavoidably result in taking decisions about the purpose and means of the processing activities[15]. The DPA further concluded that the combination of head of Compliance, Risk Management and Internal Audit within the DPO function makes it impossible to guarantee independent supervision by the DPO in each of these three departments. Moreover, the accumulation of these functions by the same individual may lead to an insufficient guarantee of confidentiality and non-disclosure vis-à-vis staff members, which comes clearly in contradiction with GDPR[16].

Another interesting element that the DPA mentioned in its reasoning was the necessity of having processes or procedures in place that an organisation should follow to anticipate and document DPO's conflicts of interest. It also implied the importance of reflecting on the role of the DPO and designing "decision trees" to facilitate and protect the impartial, consultative nature of this function while ensuring that another function or body, distinct from the DPO, will be in charge of making decisions.

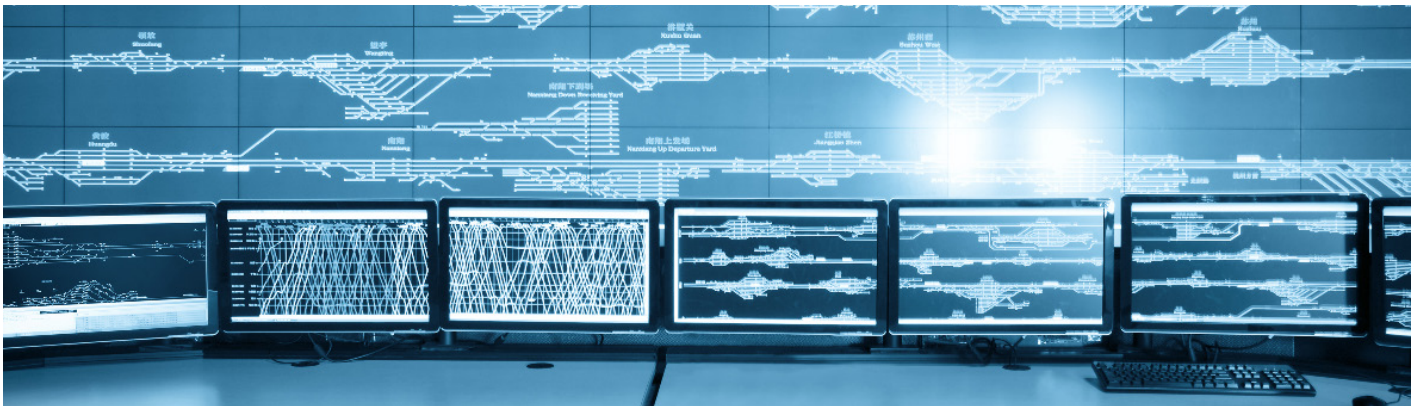
The decision also stressed the importance of having meaningful policies in place that specify the role and responsibilities of the DPO (or at large the DPO office), showing sufficiently his/her advisory regulated function that is effectively delineated from any business decision-making empowerment.

Based on the above reasoning, the Litigation Chamber finally requested the defendant to render the appointment of the DPO compliant with art. 38.6 GDPR; in other words, to ensure that the person appointed as DPO would not fulfil other duties or tasks that could result in a conflict of interest. In addition, considering the key role that the DPO is called to assume within an organisation in relation to all aspects of personal data protection, the decision has also imposed to the defendant an administrative fine of 50,000 EUR.

Although the Litigation Chamber accepted that there was no intentional violation of art. 38.6 GDPR by the defendant, it found it impossible to overlook the latter's serious failure to observe compliance with this key provision. The main arguments put forward to justify the penalty include:

The confirmation that the EU legislator awards to the DPO a key role in the Regulation; if that role is compromised, a corner-stone foundation of the GDPR is eroded.

- The concept of the DPO is not actually introduced by the GDPR for the first time; similar roles and related information and guidance on the DPO position had already existed in EU member states before the adoption of the GDPR.
- Official guidelines from the WP29 on the DPO's role had already been drafted and finalized in 2017, leaving enough time to the defendant to get familiar with the scope and practical implications of this function.
- The processing of personal data is a core activity of the defendant, which also processes personal data on a very large scale, including personal data that probably qualify as highly sensitive based on data subjects' expectations, *inter alia* because they allow for data subjects' regular and systematic observation.
- The duration of the infringement: the violation appeared to have started in 2016 and continued until 2020.



[15] On this point too, the Litigation Chamber aligns with the interpretation of the "conflict of interest" provided in the guidelines above. Those literally state that "...the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and means of the processing of personal data" (section 3.5).

[16] On this point, the decision refers explicitly to art. 38.5 GDPR: "the DPO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law".

The Role of the DPO (continued)

Practical key take-aways

While understandably the decision of the DPA came as a surprise to many, it cannot, in our view, be regarded as unreasonable. In its reasoning, the DPA clearly states that the assessment about DPO's potential conflicts of interests should be made on a case-by-case basis, taking into account the elements described above.

The combination of several "add-on" roles within the individual called to stand for the company's DPO at the same time, the nature and scale of the organisation's processing activities, as well as the size of a company and the sensitivity of the data processed, all come into play when the assessment is made.

Aligning with previous guidelines, the decision does not reject that a DPO can be a department head and even lead a large team of privacy professionals, while overseeing the work of multiple other DPOs in large corporate groups. In the same large entities, combining the DPO role with that of the head of Compliance could be problematic as in many circumstances a conflict could arise *de facto* (e.g., when the compliance officer needs to seize laptops of employees and access data to investigate anti-trust, anti-bribery and other law violations). Obviously, the assessment would be different in the case of an SME, which, due to staff and financial resources restrictions for example, would combine the roles of the DPO and head of Compliance within the same individual.

Last but not least, albeit criticized, the case is important as it is much more than only a decision on the conflict of interest ground.

It brings forward a whole analysis of key topics, ranging from the early involvement of the DPO in the data breach notification process, to practical aspects of the inspection procedure up to the data controller's duty of co-operation during the investigation. It emphasizes the importance and even obligation of any data controller to sufficiently document all data breaches as a matter of complying with data breach notification requirements but also the accountability principle at large.

On this last point in particular (accountability), the decision confirms the transversal applicability of the principle on many levels; as an obligation to demonstrate compliance with the key principles of data protection (purpose limitation, lawfulness and fairness…) but also with any of the obligations enshrined into the GDPR. As stressed in the decision and in line with the EU regulators' guidelines, the GDPR gives controllers a lot of freedom when it comes to implementation but asks evidence of compliance in return.

Our team is here to help you navigate successfully through the above issues and properly build your privacy program complied with the accountability principle and best practices relevant to the topics above.

Contacts

Anna Pouliou
Partner
Cyber and Strategic Risk
apouliou@deloitte.com
+ 32 2 600 62 39

Georgia Skouma
Director
Cyber and Strategic Risk
gskouma@deloitte.com
+ 32 2 800 24 93

Karen Van Esbroeck
Senior Consultant
Cyber and Strategic Risk
kvanesbroeck@deloitte.com
+ 32 2 301 88 96

Coryn Liesl
Senior Consultant
Cyber and Strategic Risk
lcoryn@deloitte.com
+ 32 2 302 24 60

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, tax and legal, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 312,000 professionals, all committed to becoming the standard of excellence.

Designed by CoRe Creative Services. RITM0480260.