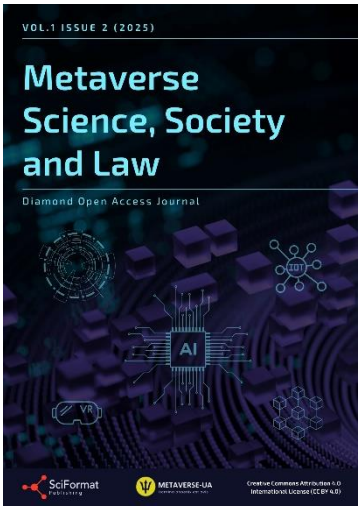

Metaverse Science, Society and Law

Vol. 1, Issue 2 (2025)

SciFormat Publishing

Publisher:
SciFormat Publishing Inc.

ISNI: 0000 0005 1449 8214
2734 17 Avenue Southwest, Calgary,
Alberta, Canada, T3E0A7

+15878858911
editorial-office@sciformat.ca

ARTICLE TITLE	GDPR PRACTICES FOR IDENTITY VERIFICATION IN THE BICYCLE RENTAL SECTOR IN BELGIUM
DOI	https://doi.org/10.69635/mssl.2025.1.2.21
RECEIVED	19 July 2025
ACCEPTED	25 September 2025
PUBLISHED	13 October 2025
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

GDPR PRACTICES FOR IDENTITY VERIFICATION IN THE BICYCLE RENTAL SECTOR IN BELGIUM

Bulgakova Daria
An Advocate, Ph.D. in International Law, Associate professor, Department of Law and Public Administration, Zaporizhzhia Institute of Economics and Information Technologies, Ukraine
ORCID ID: 0000-0002-8640-3622

ABSTRACT

This article studies the Belgian Data Protection Authority's decision of 19 August 2025 about a bicycle rental company that demanded users to provide their identity cards, where more information was placed for the contract performance, and, moreover, allowed continuous geolocation tracking. The case shows how personal data must be practically processed in compliance with the General Data Protection Regulation (GDPR). It spotlights the legal issues of necessity, legal interests, data minimization, together with the privacy, transparency, proportionality, and rights to access. The examination also stresses that location data, while not explicitly defined in the GDPR, qualifies as personal data too. The sanctions levied by the Belgian authority, including a reprimand and a warning, confirm the importance of executing robust safeguards to secure lawful processing and respect for data subjects' rights. Also, by brooding on scholarly lookouts with a practical case, the study recommends enriching identity verification practices in shared mobility services, ensuring GDPR obedience while keeping user trust.

KEYWORDS

Personal Data, Belgian Data Protection Authority, Data Protection Compliance, Identity Card, A Balancing Test

CITATION

Bulgakova Daria (2025) GDPR Practices for Identity Verification in The Bicycle Rental Sector in Belgium. *Metaverse Science, Society and Law*. Vol. 1, Issue 2. doi: 10.69635/mssl.2025.1.2.21

Introduction

The presented below case study on identity verification for bicycle rentals in Belgium is highly relevant because it reflects common practices in digital mobility services relied upon by millions of users, illustrates the application of the 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 (in the text further - GDPR)) principles to emerging technologies, provides a practical example of enforcing data protection rights in modern digital services.

The technologies described in the inventions by GUO ZIKUN et al. (2023), BU MIN et al. (2016), and YU MINMIN & WEI WEI (2017) illustrate the technical framework of shared vehicle and bicycle rental systems that rely on identity verification and user data processing. These systems collect and process personal data, including identity information, registration numbers, and location data, to verify users and control access to vehicles. All these inventions involve the collection, processing, and verification of personal data, including identity information, GPS location, and possibly other sensitive data.

In the context of the case study, such technologies highlight the potential data protection risks and the importance of GDPR compliance, particularly regarding the lawfulness, necessity, transparency, and user access to personal data processed during rental services.

The actuality of analyzing the practical case from a GDPR perspective lies in the fact that shared mobility systems, such as bicycle or vehicle rentals, heavily rely on personal data processing, including identity verification,

registration numbers, and location tracking. These processes present real-world challenges regarding the lawfulness, necessity, transparency, and security of data processing, which are core principles of the GDPR.

With regard to that, the study focuses on the following objectives:

1. Determine whether the collection and processing of identity card data and other personal information had a valid legal basis.
2. Assess whether all collected data were truly necessary for the rental service.
3. Evaluate whether users were adequately informed about how their personal data were processed, including by third-party processors.
4. Examine whether the user could exercise their right to access their data in a timely manner.

Material and Methods

The sources, legal mechanisms, and technological patents the article relied upon, and the analysis structure are as follows.

Material. For the technological set, it summarized appropriate inventions (GUO ZIKUN et al., BU MIN et al., YU MINMIN & WEI WEI), portraying bicycle rental and identity verification systems that process personal data, likewise, identity cards, GPS, and registration numbers.

For the legal framework, the GDPR (EU 2016/679), the Belgian DPA Act (2017), internal DPA rules of procedure, and EDPB guidance (2019) are functional as legal materials.

For the EU (Belgium) case study offered, Decision No. 132/2025 of the Belgian DPA refines pleadings, parties, timelines, and inquired processing practices.

Methods. It is suggested that the case study technique, when weighing a real enforcement case, looks at it as an image of how GDPR principles (lawfulness, necessity, transparency, access rights) apply to shared mobility systems.

The article laid a comparative analysis when uniting the Belgian DPA decision to the general GDPR framework and to the technological architecture of bicycle rental systems.

Also, useful doctrinal, specifically legal reasoning, because in the article, there are structured questions about valid legal basis, necessity, transparency, and access rights as analytical lenses. Interpretative method can be seen in EDPB guidance, and Court of Justice of the EU standards to assess whether the defendant's practices were law-abiding.

Results and discussion

On 19 August 2025, the Litigation Chamber of the Belgian Data Protection Authority (DPA) issued its Decision on the merits No. 132/2025. The case, registered under file number DOS-2024-01301, involved a confrontation about the illegitimate and non-transparent processing of personal data in the context of a rental contract.

The Chamber was founded on several key tools: the General Data Protection Regulation (GDPR)(EU) 2016/679, adopted on 27 April 2016; the Belgian Act of 3 December 2017, which established the DPA; and its own internal rules of procedure, authorized by the Belgian Parliament in December 2018.

The parties:

(1) On one side stood the suer, X, guided to as the complainant;

(2) On the other side was the defendant, Y, represented by counsel, Mr. Peter Craddock and Ms. Isaline d'Hoop de Synghem.

Significantly, the Litigation Chamber established that the defendant is a subsidiary of a holding company based in a neighboring country. However, the rental contract was signed in the name of the Belgian branch. The privacy notice explicitly listed the Belgian establishment as the data controller. All interactions between the complainant and the defendant took place in Belgium, and the general terms and conditions referred to the applicability of Belgian law. Therefore, the Litigation Chamber, following Article 56(2) GDPR, requested that the presumed lead supervisory authority allow the case to be handled locally in Belgium. This request was granted.

As a result, the defendant is considered the data controller for the processing of the complainant's personal data in this case.

On 10 March 2024, the complainant filed a formal objection with the DPA against the defendant.

On 2 April 2024, the DPA's Frontline Service declared the complaint admissible, and the case was then transferred to the Litigation Chamber for further handling.

On 10 June 2024, the Litigation Chamber contacted the presumed lead supervisory authority, obeying Article 56(3) GDPR, and requested permission to bear the matter locally under Article 56(2) GDPR. That submission was tolerated on 17 June 2024, which meant that the cooperation process under Article 60 GDPR did not apply in this case.

On 17 January 2025, the Litigation Chamber decided that the file was ready for a determination on the merits. The parties were formally notified by registered mail and were also informed of the deadlines for submitting their defenses.

The alleged infringements as follows:

(1) A violation of Article 5(1)(a) in intersection with Article 6(1) GDPR, for processing the complainant's self-identity card photo without a valid legal basis;

(2) A violation of Article 5(1)(c) GDPR, for processing the complainant's national register number without necessity;

(3) A violation of Article 12 in conjunction with Article 15 GDPR, for failing to grant access to the complainant's personal data after an explicit request;

(4) Violations of Articles 5(1)(a), 12, and 13 GDPR, for a lack of transparency concerning the processing of the complainant's personal data, particularly with respect to the identity card photo, the national register number, and the location data of the bicycle used by the complainant.

The merits of the case. On 7 March 2025, the Litigation Chamber received the defendant's statement of defense. On 28 March 2025, the complainant filed a reply. On 18 April 2025, the defendant submitted a rejoinder.

Position of the defendant. The defendant employs a bike rental service based on subscriptions. To use the service, a customer shall first register online. For electric bikes in particular, the customer's identity is verified after registration by sending an image of their identity card to a processor, which checks both the authenticity of the card and the accuracy of the data it holds. Only once this verification is completed can the customer schedule an appointment to collect the bike.

T*he stated purpose* of the verification is fraud prevention. When picking up the bicycle, the customer shall similarly present an identity card to prove identity, confirming that the person receiving the bike is indeed the registered subscriber.

Position of the suer. The complainant objected to this practice. She resisted having her identity card photographed both during the online verification and by a staff member at the defendant's branch office. The point specifically opposed to the back side of the card being photographed, since it controls her national register number. In accumulation, her ultimatum for access to her data was ignored, and she was not properly informed in advance about the processing of her identity card photo, her national register number, or the location data of the rented bicycle.

Questioning of the facts: data processing for the contract performance. The Chamber then turned to the principle of lawfulness, enshrined in Article 5(1)(a) GDPR. For any processing of personal data to be lawful, it must be conducted on one of the grounds listed in Article 6(1) GDPR. Article 5(2) GDPR places the burden on the controller. In this case, the defendant demonstrates compliance with this principle.

The defendant argued that the processing of customers' identity data as part of the rental process was necessary to perform the contract, relying on Article 6(1)(b) GDPR.

But to rely on contractual necessity as a legal basis, certain conditions must be met: there must be a valid contract, the contract itself must be lawful, and the processing must be objectively necessary for its performance. The European Data Protection Board (EDPB) has been clear in its guidance that simply including a reference to data processing in a contract is not enough to bring that processing within the scope of Article 6(1)(b) (EDPB, 2019].

The EDPB further stresses that the phrase "necessary for the performance of a contract" must be interpreted strictly. It does not cover situations where the processing is not truly required for the contract to be carried out, but rather unilaterally imposed on the data subject by the controller.

The Litigation Chamber first established that a contract existed between the parties and that this contract was legally valid.

The rental agreement naturally included the complainant's identity details, which were necessary for the performance of the contract.

The Chamber also noted that, both initially and after March 2024, these identity details were verified through a visual check. In practice, a staff member compared the information on the identity card with the registration data the customer had entered online. The legislator itself acknowledges the importance of this

step in laws governing the use of identity cards, because for companies and non-governmental organizations, in their dealings with citizens, it is important to have certainty about the identity of customers with whom they enter into legal relationships. A correct identity is indeed a conditio sine qua non for the legal certainty of contractual and economic relations.

Visual check of the (abundant) information on an identity card, however, is not deemed to be processing of personal data within the sense of Article 2 GDPR, since the data is not intended to be videoed in a file.

On this basis, the Chamber completed that the complainant's identity details were necessary for the execution of the rental contract, and that the defendant was therefore entitled to rely on the legal ground of Article 6(1)(b) GDPR, in line with Article 5(1)(a) GDPR, for processing the complainant's identity data as a bicycle renter.

At the time the complainant's personal data was processed, a more elaborate verification procedure was in place. This involved the use of a processor, a company specializing in identity verification software. Based on an image of the identity card, the processor checked the card's authenticity, thereby allowing the customer's identity details to be verified with greater certainty.

Unlike a straightforward visual check, this process entangles the processing of personal data within the meaning of Article 2 GDPR. It included photographing or scanning the card, filtering the data, transmitting it, checking it, storing it, and eventually deleting it. The stated purpose of this expanded verification was fraud prevention.

Even though the application used by the processor featured a privacy filter, all the personal data on the identity card was still processed, albeit briefly. The defendant itself described the situation as follows: “While a photo of an identity card is indeed analyzed in a certain way and for a very short time, this is purely to extract specific information […]” (Document 21, para 30) and “At most, the complainant could argue that there was an extremely temporary ‘processing’ before the masking effectively took place” (Document 21, para 34).

In the annex to its submissions, the defendant included an analysis of how this verification procedure operated. From this, the Litigation Chamber concluded that the photo of the identity card had to be uploaded on the defendant's website, after which it was transmitted to the processor, who only applied the privacy filter at that stage.

The defendant confirmed this in its written conclusions: “The subscriber had to take a photo of the identity card […] Once uploaded, an automatic privacy filter appeared on the photo […]” (Document 21, para 5).

Regarding the temporality of the processing, the defendant argued that it should be viewed merely as a "reading of data points" and that such a reading was permitted by law. The defendant referred to Article 6, §4 of the ID Card Act, which, however, clearly states that reading the electronic identity card must be carried out “in accordance with the legal and regulatory provisions on the protection of privacy and personal data.”

The Litigation Chamber concluded that this reading of data points constitutes processing of personal data. Accordingly, under the legislation on identity cards, it must comply with the data protection principles of the GDPR.

The matter in respect to the case study is to emphasize why the defendant’s assertion of simply "reading data points" is formidable. Data mapping indicates that any dealings with personal data (whether storing, transmitting, or accessing it, etc.) must be identified, tracked, and evaluated with data protection regulations. The Litigation Chamber’s determination that reading ID card data comprises processing aligns with this logic: if associations don’t acknowledge such shifting as processing, they risk overlooking their compliance commitments. Therefore, in cases of ambiguity, the GDPR requires proportionality to be applied (Bulgakova & Bulgakova, 2023, 67). However, if there are no viable alternatives to interference, the application of proportionality should be minimized (Bulgakova & Bulgakova V., 2023 (a), 278). In other words, the research accentuates that cognition and reasonable mapping of all data conditioning, even those that appear minimal, are compulsory to guarantee GDPR compliance. Data mapping is generally considered best practice for any data protection or privacy compliance programme, because you can’t protect your information if you don’t know:

a) that it exists,

b) where it is, and

c) the conditions under which it is kept (ITGP, 2017).

Though simply put, data mapping can prove challenging for organisations that haven’t examined their processes before, work with a great deal of personal information, or rely on data held in a variety of formats (ibid). The core compliance decision is the combination of consent validity, data processing purpose, data processing rights, and data processing operations (Chhetri, 2022, 15).

Questioning of the facts: the privacy filter. The privacy filter in the processor's application was adjustable by the data subject, which did not guarantee that the processor would not process more data than the customer's name, first name, and date of birth. It is the responsibility of the data controller to ensure that only the personal data that is necessary for processing is actually processed.

Thus, the Litigation Chamber concluded that the processing of the personal data on the identity card constitutes a separate processing of personal data, and that the use of the privacy filter alone was not an adequate technical measure to ensure that no more personal data than the name, first name, and date of birth are the data necessary for the contract were processed.

The Chamber further noted that this separate processing (carried out during the verification process) had the purpose of preventing fraud. However, as it was organized, this processing was not necessary within the contractual relationship. Initially, it was not required, and by March 2024, it was no longer being performed.

On the other side, this processing was also not necessary for the lower-cost contracts for standard bicycles. As a result, this separate processing cannot be justified based on contractual necessity under Article 6(1)(b) GDPR.

The Litigation Chamber also observed that the processing of personal data during the verification process was not based on consent (Article 6(1)(a) GDPR), not carried out to comply with a legal obligation (Article 6(1)(c) GDPR), not performed in the public interest (Article 6(1)(e) GDPR), and could not be considered vital (Article 6(1)(d) GDPR).

However, the fraud prevention could be framed as a legitimate interest under Article 6(1)(f) GDPR, namely the defendant's interest in avoiding economic loss.

The defendant's privacy statement explicitly refers to its legitimate interest in preventing fraud. It highlights that ensuring a rented bicycle, particularly a high-value electric bike, is handed over to the correct person is central to the service. The privacy statement also outlines this interest among the purposes of processing personal data. In its submissions, the defendant emphasized that this verification process is essential for fraud prevention. And, it may be taken into account because the risk-based approach in the GDPR suggests a layered analysis of vulnerability: everyone is potentially vulnerable, but at varying levels and contexts (Malgieri, 2023, 90).

Questioning of the facts: a legitimate interest. Recital 47 of the GDPR specifically states that direct marketing is a legitimate interest, subject to a three-part balancing test (Harris et al. 2018). Ideally, theinterests of the practice, client andwider society should coincide as theywould for the marketing of products orservices, for example (ibid). According to established case law practice of the Court of Justice of the European Union regarding legitimate interests, a controller must demonstrate three things:

(1) the interest it seeks to protect is indeed legitimate,
(2) the processing is necessary to achieve that interest, and
(3) a balancing test favors the controller's interest over the rights and freedoms of the data subject.

The Litigation Chamber observed that the defendant had not provided such a balancing test. To assess whether the legitimate interest could constitute a proper legal basis, the Chamber conducted the balancing itself.

First, looking at the purpose, the Chamber considered that because the bicycles are only rented and remain the property of the defendant, preventing fraud and ensuring that the bicycle is handed to the correct person clearly constitutes a legitimate interest.

Second, the Chamber examined whether the processing was necessary. For processing to be necessary, it must be suitable, adequate, and indispensable for achieving the intended purpose.

There is no doubt that an identity card is particularly suitable for verifying a person's identity and adequate for confirming it with certainty. Identity cards are designed and secured specifically for this purpose.

Accordingly, processing by analyzing data points from a photo or scan of the identity card is also adequate. However, this analysis involves photographing or scanning the identity card, transmitting the image over the internet, and then storing, and deleting it. Each of these steps increases the risk of errors or potential breaches of the confidentiality or integrity of all the data on the card. This processing was not necessary because a simpler alternative already existed. The defendant had a procedure in place that involved physically comparing the registration details entered online by the customer with the identity card in the store before handing over the bicycle. This procedure was reinstated in March 2024 because processing via a photo or scan of the identity card added no meaningful value to the purpose of fraud prevention.

Since the three conditions for lawful processing under legitimate interest are cumulative, and because the processing was not necessary, the Litigation Chamber concluded that the defendant could not rely on legitimate interest to process the personal data on the complainant's identity card.

The Chamber determined that the defendant breached the GDPR, specifically Article 5(1)(a) in conjunction with Article 6(1), by lacking a legal basis for processing the personal data on the complainant's identity card.

Questioning of the facts: unnecessary data processing. The complainant objected to photographing and uploading her identity card, arguing in particular that processing her national register number was unnecessary. She did not, however, oppose a simple check of her identity card to compare the information with the registration details already held by the defendant. In her view, this form of verification was sufficient.

The Litigation Chamber noted that the alleged processing of the national register number was part of the broader identity card verification procedure. Since this verification procedure had already been deemed unlawful, any processing of the national register number was likewise unlawful. As a result, there was no need to separately assess compliance with the principle of data minimization, because the underlying processing itself was already invalid.

The complainant stated that she was never directly informed about the processing of her personal data. She had to search online for the privacy statement herself to obtain information about how her data would be processed.

The defendant showed that the rental contract included a link to the privacy policy and that the privacy statement was also available on the website used for registering for the bicycle rental. At the same time, study shows, several websites made it rather complicated for users to find these links as they, for example, had a privacy policy link in the site's footer but used infinite scrolling to dynamically add more content when the user scrolled to the bottom of the page, moving the footer out of the visible area again (Degeling et al., 2019, 4). Also, the time and effort required to read and understand the information on cookie banners, coupled with the need to make multiple decisions, can be burdensome for users (Porcelli, et al., 2024, 4). This may explain why even users who claim to be concerned about their privacy accept all tracking cookies at the same time—this is the so-called privacy paradox (ibid).

The Litigation Chamber concluded that the complainant had been sufficiently informed in advance about the existence of the privacy statement and where to find it. However, while the privacy statement mentioned the processing of identity data, it did not include the use of the identity card in the verification procedure, even though this constituted a separate processing activity. Moreover, the processor conducting this verification was not named in the privacy statement, which only referred to processors in a more general context. The Chamber noted that this specific processing was explicitly mentioned in the general terms and conditions, but because this information was in a separate document, it violated the principle of transparency under GDPR. Therefore, institutions should respect and sustain different practices, such as presenting information in a layered format or providing summaries of key highlights upfront (Bulgakova & Bulgakova, 2024, 95).

Regarding the processing of the national register number, which appears on the back of the complainant's identity card, the privacy statement contained no information. This aligns with the defendant's argument that only the front of the identity card was processed. Furthermore, the complainant did not demonstrate that the back of the card had been processed, and this can no longer be verified, as all personal data held by the processor had reportedly been deleted since March 2024. In that means, splitting the information between the privacy statement and the general terms creates confusion and a lack of clarity, which undermines transparency. At the same time, the GDPR intentionally does not specify any design template or rules, and thus leaves the exploration of the design space for consent dialogs to the market participants (Machuletz & Böhme, 2020, 482).

Questioning of the facts: transparency lack. Concerning the processing of the bicycle's location data, the privacy statement mentions that the last known location may be used to recover a lost or stolen bicycle or in the case of non-payment. It clarifies this purpose, but the statement does not specify whether location data may be collected occasionally, randomly, or continuously. The fact that location data can be continuously tracked implies the presence of a tracker in the bicycle. By only mentioning its use in case of problems, the defendant failed to provide transparency about potential tracking when no problems occurred.

The Litigation Chamber concluded that the defendant violated the principle of transparency under Article 5(1)(a) in conjunction with Articles 12 and 13 of the GDPR. The violation arises because the processing of the identity card by a processor was not mentioned in the privacy statement, and it was unclear whether the bicycle tracker collected location data even when no issues had been detected. In terms of bicycle tracker – it is significant to differentiate the status of such a third-party. In the context of third-party tracking, the first party (e.g. the app developer) is likely a controller; the third parties may be processors (where they only process data on behalf of the first party, e.g. for app analytics), controllers in their own right (where they use the first-party data for their own purposes such as targeted advertising, improving their machine learning models, etc.),

or sometimes both at the same time (Kollnig et all., 2021, 3). This counts because the legal burdens under GDPR lean on whether the third party is serving as a processor (only abiding by data for the app developer) or as a controller (using the data for its own intents, like advertisement or AI practicum). If the functions aren't clearly expressed and proclaimed, users don't know who is liable for their data or how it will be used (which straight sabotages transparency and accountability).

Questioning of the facts: right of access. Article 12 of the GDPR describes what controllers have to do in terms of providing data subjects with information about the processing that is to occur, and about making them aware of their rights (Governance, 2019). Article 12.1 of the GDPR requires that information about data processing be concise and easily accessible.

In this regard, the Chamber examined the complainant's right of access. Under the GDPR, every data subject has the right to obtain confirmation from the data controller about whether their personal data is being processed, and if so, to access that data. The controller must also provide a copy of the personal data being processed.

The GDPR further sets out how data subjects can exercise these rights. Controllers are required to facilitate the exercise of rights and provide information on the measures taken in response to a request without undue delay and in any case within one month. It is especially important because consenting the use of personal data is an ongoing process and organizations must be able to review regularly whether those that they hold personal data on and use are happy for that to continue (Laybats & Davies, 2018, 81). So, in the view of the study, such pleas, rather than being seen just as a responsibility to reply, truthfully provide businesses with a worthwhile instrument to carry out this persistent reexamination of consent.

If the controller does not act on the request, the data subject must be informed without delay, and at the latest within one month, of the reasons why the request was not followed, as well as their right to lodge a complaint with a supervisory authority or to seek judicial remedy.

As part of her complaint, the complainant attached an email dated 14 January 2024, in which she requested access to all personal data that had ever been collected or processed about her. The Litigation Chamber noted from the case file that no access was granted within the one month required by GDPR, nor did the defendant request an extension of that period.

The defendant argued that the request had ended up in their spam folder and was only discovered after the Chamber's invitation to submit conclusions on 17 January 2025 (a full year later).

The Chamber observed that this delay prevented the complainant from verifying whether her national register number had been processed, whether the photo of her identity card had been deleted, or whether location data from her bicycle rides had been recorded.

The Chamber concluded that the defendant violated the complainant's right of access under Articles 12 and 15 of the GDPR by failing to provide access to her personal data following her explicit request within the required one-month timeframe.

The severity of the breach. The Litigation Chamber considered the seriousness of the breach. It emphasized that the principle of lawfulness is a fundamental cornerstone of the protection guaranteed by the GDPR and is also enshrined in Article 8.2 of the Charter of Fundamental Rights of the European Union. Violations of this core principle are therefore serious. Hence, in such scenarios, an organisation must have a mechanism for notifying its local supervisory authority in case of a data breach, it must appoint a data protection officer, and it must be able to document that its systems comply with best IT-security practices (Arfelt et al., 2019, 686).

The defendant's failure to include the disputed processing in the privacy statement, combined with the failure to respect the complainant's right of access within the required timeframe, made it impossible for the complainant to verify whether her personal data were adequately protected. This lack of oversight rendered the complaint inevitable.

At the same time, the Chamber noted mitigating factors. The disputed processing had been temporary and had already been stopped voluntarily in March 2024, including the deletion of the data collected during that processing. The defendant had also implemented technical measures to limit the processing, although these measures were not fully sufficient.

Besides, the Chamber took into account that the access request was eventually fulfilled, and that the processing of location data was mentioned in the privacy statement, even if the explanation provided did not fully guarantee clarity regarding the processing.

The Litigation Chamber decided to reprimand the defendant for the following:
(1) Processing the complainant's identity card data without a legal basis;
(2) Failing to respond to a lawful access request from the complainant within the required timeframe;
(3) Lack of transparency regarding the processing of the identity card data by a processor.

Also, the Chamber decided to issue a warning to the defendant regarding the lack of transparency in processing the bicycle's location data. While it was clear to the complainant that location data were being processed, it was unclear whether this data were tracked continuously, creating a transparency issue.

Conclusions

The European data protection framework acknowledges two categories of data: personal and non-personal data (Finck & Pallas, 2020, 13). Although the GDPR is a multifaceted regulation, many of its elements support the GDPR's key principle of data minimization: Firms must limit the personal data that they process ((Johnson et al., 2023, 5698). Firms must audit internal data processes, encrypt and anonymize personal data, and notify affected individuals and the regulator in the event of a data breach (ibid). Firms are also responsible for respecting the new data rights of EU residents under the GDPR, including the rights to: access personal data, correct data, erase data, transfer data, and object to data processing (ibid). In sum, the GDPR incentivizes firms to limit personal data processing by increasing both its associated operational cost and legal liability (ibid).

The studied case demonstrates that identity data and location data processed in the context of shared mobility services fall within the GDPR's scope of application, therefore, are a personal data. As Dibble (2020) notes, when looking at whether the information in question falls within the scope of personal data, you need to look at the nature, content, and format of that information. Also the author thinks, location data isn't specifically defined in the GDPR, nor does it provide any specific guidance on how to deal with it [ibid]. If the location data is processed with other information relating to an individual, the device, or the individual's behavior, or is used in a way to single out one individual from others, it's personal data even if identifiers such as name and address are not known [ibid]. In certain circumstances, location data could reveal special-category data; for example, if the individual has visited hospitals or places of worship or has been present at political demonstrations [ibid]. This strengthens the Litigation Chamber's result that geolocation and identity card verification demand strong safeguards of lawfulness, transparency, and proportionality. Moreover, users should be given clear and intelligible information about how their data will be used, who will have access to it, and any potential dangers connected with giving it (Pinto, 2024).

The conclusion of the Belgian DPA's decision exemplifies how defeats in transparency and punctual access rights damage user trust and GDPR obedience. As Hansen characterizes with the model of age-verification systems, consistent data-minimizing courses must be carefully devised to protect fundamental rights. For example, an age verification profile where only the date of birth and the portrait picture are accessible (for the disco bouncer use case) (Hansen, 2018, 359).

Taken above for the consideration, it is clear that the Litigation Chamber of the Belgian DPA administered a reprimand for wrongful processing of identity card data without a reasonable legal foundation, loss to answer to the complainant's access request within the demanded timeframe, and absence of translucence about identity card verification by a processor. Also, the Chamber bore a forewarning concerning the deficiency of clarity in processing location data.

GDPR removes the need for an independent basis and provides a formalized remedy for noncompliance (Sharma & Menon, 2020). In this regard, the case study pictures that identity verification procedures and location tracking in bicycle rental assistance are not just specialized components, but legal touchpoints where GDPR principles such as lawfulness, necessity, transparency, and user rights must be executed rigidly to conserve individual privileges in a data-driven society.

Acknowledgements: None.
Funding: The study was not funded.
Conflict of interest: None.

REFERENCES

1. Arfelt, E., Basin, D., & Debois, S. (2019). Monitoring the GDPR. In P. Y. A. Ryan, S. Schneider, & K. Sako (Eds.), *Computer Security - ESORICS 2019* (Vol. 11735, pp. 681–699). Springer International Publishing AG. https://doi.org/10.1007/978-3-030-29959-0_33
2. BU MIN, JIANG YINGHONG, WANG XIAOJUN, & PENG QINGYAN. (2016). *Public bicycle renting personal terminal service system*.
3. Bulgakova D., Bulgakova V. (2024). Facial Recognition at the Fitness Center Under the General Data Protection Regulation Article 9(1) and 9(2)(a). Jiao da fa xue ping lun NCTU law review, 14, 61–97. https://lawreview.law.nycu.edu.tw/lawreviewlaw/ch/app/data/view?module=nycu0040&id=33646&serno=d8011b0c-b400-4f87-83ba-9c2e85dfd61c
4. Bulgakova, D., & Bulgakova, V. (2023). The Compliance of Facial Processing in France with the Article 9 Paragraph 2 (a) (g) of (EU) General Data Protection Regulation. *Naukovì Zapiski NaUKMA. Ûridičnì Nauki*, *11*, 64–76. https://doi.org/10.18523/2617-2607.2023.11.64-76
5. Bulgakova D., Bulgakova V. (2023 (a)). The processing of personal data in accordance with the principle of proportionality under the EU General Data Protection Regulation. PHILOSOPHY, ECONOMICS AND LAW REVIEW, 3 (1), 266 - 284. https://phelr.dduvs.edu.ua/? page_id=3199
6. Chhetri, T. R., Kurteva, A., DeLong, R. J., Hilscher, R., Korte, K., & Fensel, A. (2022). Data Protection by Design Tool for Automated GDPR Compliance Verification Based on Semantically Modeled Informed Consent. *Sensors (Basel, Switzerland)*, *22*(7), 2763. https://doi.org/10.3390/s22072763
7. Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). *We Value Your Privacy... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy*. https://doi.org/10.48550/arxiv.1808.05096
8. Dibble, S. (2020). *GDPR for dummies* (1st edition). For Dummies.
9. Document 21, Summary Conclusion, and Additional Document of 18 April 2025.
10. EDPB, Guidelines of 8 October 2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, version 2.0, paragraph 26.
11. Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11–36. https://doi.org/10.1093/idpl/ipz026
12. Governance, I. (2019). *EU General Data Protection Regulation (GDPR), third edition - An Implementation and Compliance Guide* (1st edition). IT Governance Publishing.
13. GUO ZIKUN, DU HONGLEI, MA TAO, JIA PEIQI, GAO CHAO, CUI PENGFEI, YAN LEI, LI YONGCHUN, ZHANG XIN, CHEN LINA, & HU YONGQING. (2023). *Self-service bicycle taking and returning method, device and system based on shared bicycle and user mobile terminal*.
14. Hansen, Marit., Kosta, Eleni., Nai-Fovino, Igor., & Fischer-Hübner, Simone. (Eds.). (2018). *Privacy and Identity Management. The Smart Revolution : 12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Ispra, Italy, September 4-8, 2017, Revised Selected Papers* (1st ed. 2018.). Springer International Publishing. https://doi.org/10.1007/978-3-319-92925-5
15. Harris, D., Samuel, S., & Probert, E. (2018). GDPR confusion. *Veterinary Record*, *183*(12), 388–388. https://doi.org/10.1136/vr.k3956
16. ITGP Privacy Team. (2017). *EU General Data Protection Regulation (GDPR) : an implementation and compliance guide* (2nd ed). IT Governance Publishing.
17. Johnson, G. A., Shriver, S. K., & Goldberg, S. G. (2023). Privacy and Market Concentration: Intended and Unintended Consequences of the GDPR. *Management Science*, *69*(10), 5695–5721. https://doi.org/10.1287/mnsc.2023.4709
18. Kollnig, K., Binns, R., Van Kleek, M., Zhao, J., Lyngs, U., Tinsman, C., & Shadbolt, N. (2021). Before and after GDPR: Tracking in mobile apps. *Internet Policy Review*, *10*(4), 1–30. https://doi.org/10.14763/2021.4.1611
19. Laybats Claire, & Davies, J. (2018). GDPR. *Business Information Review*, *35*(2), 81–83. https://doi.org/10.1177/0266382118777808
20. Litigation Chamber of the Belgian Data Protection Authority (DPA), Decision on the merits No. 132/2025, the case no. DOS-2024-01301, 19 August 2025, https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-132-2025.pdf
21. Machuletz, D., & Böhme, R. (2020). *Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR*. https://doi.org/10.48550/arxiv.1908.10048
22. Malgieri, G. (2023). *Vulnerability and data protection law* (First edition.). Oxford University Press. https://doi.org/10.1093/oso/9780192870339.001.0001
23. Pinto, R. (2024). Part 4 - Digital Identity Era: A Probabilistic Future. In *Decentralized Identity Explained*. Packt Publishing, Limited.
24. Porcelli, L., Mastroianni, M., Ficco, M., & Palmieri, F. (2024). A User-Centered Privacy Policy Management System for Automatic Consent on Cookie Banners. *Computers (Basel)*, *13*(2), 43. https://doi.org/10.3390/computers13020043

25. 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). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
26. Sharma, S., & Menon, P. (2020). *Data privacy and GDPR handbook* (1st edition). John Wiley & Sons.
27. The DPA Act, https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2017120311&table_name=wetYUMINMIN&WEIWEI. (2017). *Public bicycle rental system and its control method and device*.