

## Decision

### Complaint regarding the right to access

A complaint was lodged with my Office, on 25/11/2022, on behalf of XXXX against Brivio Limited, regarding the right of access (Article 15 of the GDPR).

#### **1. Description of the case**

1.1. The complaint was lodged on 25/11/2022, by XXXX (hereinafter, “the Law Firm”) on behalf of XXXX (hereinafter, “the Complainant”) against Brivio Limited (hereinafter, “the Controller”) and involves the Controller’s failure to comply with the Complainant’s access request.

1.2. Since the attached, to the complaint form, written request to the Controller, was in German, the Commissioner, on 30/12/2022, asked the Complainant to provide the Greek or English version of the said document in order to be able to investigate the complaint. On 10/01/2023, the Commissioner received an English translation of the complaint.

1.3. According to the Complainant, he had been a customer of the Controller. The former contacted the latter via the Law Firm, at the postal address “Office 102, 12A Lekorpouzier, 3075 Limassol, Zypern” on 10.10.2022, requesting that the Controller provides him with “cost-free and complete (including data regarding other websites) information” regarding the payment and gaming history, as well as all other personal data relating to him, as was his legal right according to Article 15 of the General Data Protection Regulation (EU) 2016/679 (hereinafter, “the GDPR”). He requested the said information to be delivered to the legal office within one month at the latest.

1.4. Moreover, information about the following questions was requested in case the Controller processed personal data of the Complainant:

- “1. What personal data do you process?*
- 2. For what purpose(s) do you process this data?*
- 3. Where does this data come from?*
- 4. Have you transferred or do you plan to transfer these data to third parties? If yes, to whom, when and for what purpose(s)?*
- 5. Send us the complete payment and gaming history of all gaming accounts of our clients in machine-readable excel format.*
- 6. How long will you process the data (data deletion concept)?*
- 7. Have you created a profile regarding our client? If yes, please tell us the content of this profile and how it was created”.*

1.5. Nevertheless, the Complainant claimed that he had not received any response to his request despite the deadline and the documented delivery.

#### **2. Investigation by Cyprus SA**

2.1. The Commissioner contacted the Controller on 19/01/2023 and requested the reason for not responding to the Complainant’s access request as well as any other information they

deemed necessary. The Controller was also informed for the provisions of the Articles 15(1) and 12(3) of the GDPR.

2.2. In their reply, on 31/01/2023, the Controller stated, inter alia, the following:

- i. On 24/10/2022, the Controller received at their postal address (Office 102, 12A Lekorpouzier, 3075 Limassol, Zypern) a letter from the Law Firm requesting access to personal data of the Complainant according to Article 15 of the GDPR.
- ii. The Controller's internal investigation has determined that a failure by a staff member responsible for registering incoming correspondence and redirecting it to the relevant departments and officers was the reason for the non-answering within the one-month period.
- iii. However, the Controller noted that they were experiencing a higher-than-normal volume of data subjects' requests (DSARs). During the period of October 2022 to January 2023, they received twenty-seven DSARs at their postal address and ten DSARs at their e-mail address dedicated to privacy matters, from the Law Firm, all on behalf of different data subjects.
- iv. The Controller fully complied with all of the DSARs received from the Law Firm, providing all necessary information in a timely manner. This statistic shows that their commitment to fulfilling data protection obligations is a top priority, and they continue to work closely with the Law Firm to ensure the accurate processing of their DSARs.
- v. The Controller has taken all reasonable measures to allow data subjects to exercise their rights in accordance with the GDPR. Despite all their employees being well qualified and trained, in some cases, they cannot completely prevent a human error that is generally common in the person's behaviour, especially when faced with a high volume of DSARs from one law firm.
- vi. Upon receipt of the complaint, the Controller's Data Protection Team immediately reached out to the Law Firm. On 19/01/2023, they sent personal data of the Complainant to the Law Firm and answered to the questions regarding their privacy practices.
- vii. The Controller conducted additional explanatory sessions for their team on the proper fulfilment of their professional duties and implemented additional supervision in the correspondence management process.

2.3. Moreover, the Controller asked for the Commissioner's expert advice regarding the DSARs submitted by the Law Firm and mentioned, inter alia, the following:

Taking into account the number, frequency, and purpose of DSARs submitted by the Law Firm on behalf of their clients, the Controller believes that they have all reasonable grounds to consider these requests "manifestly unfounded" under the GDPR. The Controller has several factors that they consider to be evidence of the abuse of data subject rights as granted by the GDPR:

- i. Using the right of access for purposes that are not related to data protection:
  - the Law Firm acts as a legal representative of the Controller's customers who are dissatisfied with the latter's services and seeking reimbursement. For this purpose, the Law Firm submits DSARs prior to making any legal complaints or demands.

- According to Recital 63 of the GDPR, Art. 15 of the GDPR grants the data subject a right “to be aware of, and verify, the lawfulness of the processing”. In the current situation, considering all circumstances, it can be argued that the intention of the Law Firm is not to actually verify the lawfulness of the processing.
  - For clarity, it is worth mentioning that shortly after complying with DSARs, the Controller often receives claims for reimbursement on behalf of the relevant customer with a warning to file a lawsuit with court in case of failure to satisfy the claims. This implies that the Law Firm has motives that are unrelated to data protection and privacy.
  - The Controller assumes that the goal of the data subject requests submitted by the Law Firm is not to exercise the right of access as outlined in Article 15 of the GDPR, but rather to fish for legal opportunities, use the information against the Controller and gain financial benefits. This makes the baseless nature of the DSARs clear and obvious.
- ii. Number and frequency of DSARs:

- the Law Firm submitted over thirty-five DSARs on behalf of different data subjects to the Controller between October 2022 and January 2023, using both the Controller’s postal and privacy email address. Such a high volume of requests not only causes disruption and places an excessive burden on the Controller to respond, but also creates potential legal and compliance risks.
- As demonstrated, there are reasonable grounds to consider DSARs submitted by the Law Firm as “manifestly unfounded”:
  - the Law Firm has no genuine interest in exercising the right of access on behalf of its customers and is instead exploiting its formal legal position to use DSARs as means of disrupting the business activity of the Controller;
  - the Law Firm is targeting our Company on behalf of data subjects who are left dissatisfied with our services;
  - the Law Firm systematically sends identical requests on behalf of different data subjects as part of a campaign.
- The Controller makes all reasonable efforts to comply with its obligation under the GDPR to facilitate the exercise of data subjects’ rights. Despite the manifestly unfounded nature of these requests, we have never refused the Law Firm’s requests for a copy of the personal data. However, the number of requests from the Law Firm continues to grow, putting an increasing burden on the Controller in terms of time and resources.
- Given that the threshold for recognizing data subject requests as “manifestly unfounded” under the GDPR is too vague and that we were not able to find any specific guidelines of the Commissioner in this regard, we are seeking the Commissioner’s expert advice on whether we can refuse future DSARs from the Law Firm due to their manifestly unfounded nature.

2.4. On 28/06/2023, the Commissioner contacted the Law Firm and asked them to confirm whether the access request had indeed been satisfied.

2.5. Also, on 05/09/2023, the Commissioner asked the Controller to provide evidence regarding their position that both the Complainant’s personal data and answers to questions about the Controller’s privacy practices had been sent to the Law Firm.

2.6. The Controller replied on 22/09/2023, repeated the content of its previous letter and attached the following files:

- i. An email from the Controller to the Law Firm says, inter alia, that a copy of the Complainant's personal data as well as answers to the questions regarding the Controller's practices for processing personal data are sent. It appears that four files were attached to this email.
- ii. The Controller shared with the Commissioner's Office, a record with title "Data Subject Access Requests Obtained from the Law Firm during the period of October 2022 to January 2023", including the date of receiving, the reference number of each request, the response date and the source (email or postal address), as well as screenshots of each data subject request and the response from the Controller. As the latter mentions, "Detailed information regarding the receipt and timely response to each request is available in the Evidence 2' file accompanying this letter".

2.7. On 01/11/2023, the Commissioner received a confirmation from the Law Firm that the requested information was fulfilled in January 2023.

### **3. Preliminary Decision**

3.1. In view of all the information provided before the Commissioner and pursuant to the Articles 58 and 83 GDPR, on 17/11/2023, the Commissioner issued a Preliminary Decision, according to which there was an infringement of the Article 12(3) GDPR, on behalf of the Controller, since the latter failed to respond to the Complainant's access request within the one-month period and, hence, to comply with the provisions of the aforementioned Article. The Preliminary Decision was notified to the Controller, at the aforementioned date.

3.2. Moreover, the Controller was informed that, based on the provisions of Article 58(2) GDPR, the Commissioner has the authority to impose an administrative fine pursuant to Article 83 GDPR. The Controller was given the right to be heard provided by Article 43 of the General Administrative Law Principles Law of 1999, of Law 158(I)/1999, as amended and invited, by 15/12/2023 at the latest, to state reasons why they believe they should not be sanctioned and/or any mitigating factors that they believe should have been taken into account before a Decision was issued. Also, they were requested to inform the Commissioner about their turnover for the previous financial year.

3.3. On 14/12/2023, the Controller responded to the Preliminary Decision and stated, inter alia, the following:

- i. In the recent case *Lees v Lloyds Bank Plc* EWHC 2249 (Ch) (24 August 2020) that occurred in the United Kingdom, the claimant submitted multiple DSARs to the bank regarding his properties. The bank failed to respond to some of the DSARs within the stipulated one-month period. Moreover, the claimant was dissatisfied with the responses to certain DSARs, leading him to take the matter to court. The court decided that the claim was without merit and should be dismissed. In reaching the final decision, the court considered the following factors:
  - The issue of numerous and repetitive DSARs which is abusive;
  - The real purpose of the DSARs was to obtain documents rather than personal data;
  - There was a collateral purpose that lay behind the requests which was to obtain assistance in preventing the bank from bringing claims for possession. A collateral purpose of assisting in litigation is not an absolute answer to there

being an obligation to answer a DSAR, but it is a relevant factor in the exercise of the court's discretion;

- The fact that the data sought will be of no benefit to the claimant. The claims for possession have been the subject of final determinations in the County Court from which all available avenues of appeal have been exhausted.
- ii. Keeping in mind the court's conclusion, the following refer to "the DSAR submitted by the Law Firm":
- **Abusive Nature of DSAR:** The number and repetitive nature of the DSARs submitted by the Law Firm were highly unusual and abusive. The volume and frequency of the requests exceeded what is typically considered reasonable for a DSAR. Detailed evidence of the frequency / excessive nature of these requests, has been provided to the Commissioner in their previous correspondence.
  - **Real Purpose of DSARs for Legal Procedures:** The real intent behind the DSAR in question was not a genuine interest in personal data access as intended by the GDPR, but rather an attempt to gather information for potential litigation. This misuse of DSARs as a legal tool detracts from their intended purpose of protecting individual data rights, as outlined in the GDPR's principles of fairness and transparency.
  - **Collateral Purpose for Legal Proceedings:** The collateral purpose of the DSAR was to acquire documents to assist the lawyer's position in potential legal proceedings against our company.
- iii. Emerging trends in data protection regulation, such as those reflected in the UK's draft Data Protection and Digital Information Bill, propose to categorize certain DSARs as "vexatious" if they constitute "an abuse of process". This bill reflects new "best practices" in regulatory approaches that acknowledge the importance of assessing the intent behind DSARs when determining compliance and sanctions. This reflects a growing recognition in the field of data protection that the right of access must be balanced against misuse for unrelated purposes. This evolving perspective is in harmony with the GDPR's commitment to reasonable and fair data processing.
- iv. In light of these factors, the DSAR submitted by the Law Firm was not motivated by genuine privacy concerns but rather served as a pre-litigation disclosure exercise. As such, there has been no serious breach of user privacy rights.
- v. The turnover of the Controller, for the financial year, is 321.649 EUR.

## **4. Legal framework**

### 4.1. Article 58 of the GDPR:

"1. Each supervisory authority shall have all of the following investigative powers:  
(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks; [...]

2. Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

- (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
- (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
- (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period; [...]
- (f) to impose a temporary or definitive limitation including a ban on processing; [...]
- (i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case; [...]"

#### 4.2. Article 15 of the GDPR:

"1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- (a) the purposes of the processing;
- (b) the categories of personal data concerned;
- (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- (f) the right to lodge a complaint with a supervisory authority;
- (g) where the personal data are not collected from the data subject, any available information as to their source;
- (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. [...]

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form".

#### 4.3. Article 12(3) of the GDPR:

"The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. [...]"

#### 4.4. Article 83 of the GDPR:

"1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

- (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
- (b) the intentional or negligent character of the infringement;
- (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
- (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
- (e) any relevant previous infringements by the controller or processor;
- (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
- (g) the categories of personal data affected by the infringement;
- (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
- (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
- (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
- (k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement. [...]

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
- (b) the data subjects' rights pursuant to Articles 12 to 22;
- (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
- (d) any obligations pursuant to Member State law adopted under Chapter IX;
- (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. [...]"

## **5. Views of the Commissioner**

5.1.1. Considering all the information above, the Controller failed to comply with the provisions of the Article 12(3) since they did not respond to the Complainant's access request within the aforementioned one-month period.

5.1.2. I take into account that the Controller, shortly after being informed that the Complainant lodged a complaint with my Office, reached out to the latter and completely fulfilled his request. Nevertheless, I consider that, the Controller understands that the request could have been satisfied from the first instance if the appropriate organizational and technical measures were in place and the staff was properly trained in dealing with GDPR requests in a timely manner.

At this point, I wish to respond to the Controller's allegations, by referring to the Guidelines 01/2022 on data subject rights - Right of access (Version 2.0), adopted on 28/03/2023:

### 5.2. Regarding the claimed "manifestly unfounded" nature of the DSARs submitted by the Law Firm on behalf of their clients:

5.2.1. The Controller asked for the Commissioner's expert advice regarding the "manifestly unfounded" nature of the DSARs submitted by the Law Firm for the following reasons:

- I. the Law Firm has no genuine interest in exercising the right of access on behalf of its customers and is instead exploiting its formal legal position to use DSARs as means of disrupting the business activity of the Controller;
- II. the Law Firm is targeting the Controller on behalf of data subjects who are left dissatisfied with our services;
- III. the Law Firm systematically sends identical requests on behalf of different data subjects as part of a campaign.

5.2.2. The term "manifestly unfounded" can be found in the Article 12(5) of the GDPR, according to which: "Where requests from a data subject are manifestly unfounded or excessive, **in particular because of their repetitive character**, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request".

5.2.3. I wish to clarify that the Article 12(5) refers to the case when a **single data subject** submits a request or several requests and this/these request(s) is/are considered manifestly unfounded. Therefore, I cannot answer to the Controller's question regarding the "manifestly unfounded" nature of the DSARs submitted by the Law Firm, **as a whole**, since those requests were all submitted on behalf of **multiple different data subjects**, regardless of the fact that the said data subjects were represented by the same law firm. "41. When receiving requests for access to personal data, the controller **must assess each request individually**", as follows by the Guidelines 01/2022.

### 5.3. Regarding the DSAR submitted by the Complainant:

5.3.1. According to the Guidelines 01/2022:

**"177. A request for the right of access is manifestly unfounded, if the requirements of Art. 15 GDPR are clearly and obviously not met when applying an objective approach [...]"**.

5.3.2. The Complainant requested to be provided with the personal data processed by the Controller concerning him and answers to questions about the Controller's privacy practices. It appears that, the Complainant's request was in line with the Article 15 of the GDPR.



5.3.3. Regarding the purpose / intention behind the submission of DSARs by the Law Firm and the refer to the UK's draft Data Protection and Digital Information Bill, I wish to mention that, regarding the Complainant's DSAR, the Controller could not know with certainty in advance whether the Complainant would proceed with the use of the information against the former in order to gain financial benefits. At least, at the time of the submission of the Complainant's request, there did not appear to be such intention. Despite the fact that, after complying with DSARs submitted by the Law Firm, the Controller often receives claims for reimbursement on behalf of the relevant customer, this does not mean that, in the case of the Complainant, the same would be the case.

5.3.4. In any case and according to the Guidelines 01/2022:

“13. Given the broad aim of the right of access, **the aim of the right of access is not suitable to be analysed as a precondition for the exercise of the right of access by the controller** as part of its assessment of access requests. Thus, controllers should not assess “why” the data subject is requesting access, but only “what” the data subject is requesting [...] and whether they hold personal data relating to that individual [...]. Therefore, for example, **the controller should not deny access on the grounds or the suspicion that the requested data could be used by the data subject to defend themselves in court** in the event of a dismissal or a commercial dispute with the controller.

Example 1: An employer dismissed an individual. One week later, the individual decides to collect evidence to file an unfair dismissal lawsuit against this former employer. With that in mind, the individual writes to the former employer requesting access to all personal data relating to him or her, as data subject, that the former employer, as controller, processes.

The controller shall not assess the intention of the data subject, and the data subject does not need to provide the controller with the reason for the request. Therefore, if the request fulfils all other requirements (see section 3), the controller needs to comply with the request, unless the request proves to be manifestly unfounded or excessive in accordance with Art. 12 (5) of the GDPR (see section 6.3), which the controller is required to demonstrate”.

5.3.5. In view of the above, the Controller's position regarding the purpose / intention behind the DSARs submitted by the Law Firm or behind the DSAR submitted on behalf of the Complainant, cannot be considered.

5.3.6. Regarding the claimed higher-than-normal volume of identical DSARs submitted by the Law Firm, I wish to mention that this **should not had affected the Controller's ability to respond to the Complainant's DSAR in a timely manner**. The DSARs were all submitted on behalf of different data subjects; the fact that the said data subjects were represented by the same law firm does not make any difference.

5.3.7. Therefore, I cannot take into account the allegations regarding the high volume of submitted DSARs by the Law Firm.

5.3.8. Furthermore, as regards to the case *Lees v Lloyds Bank Plc* EWHC 2249 (Ch) that occurred in the UK and which the Controller is referring to, cannot be taken into consideration. The case refers to a single data subject who had submitted multiple DSARs. The court considered the numerous and repetitive DSARs abusive, which is not the case, in this particular complaint. The current complaint refers to the submission of a single DSAR on behalf of a single data subject (the Complainant). Also, the court took into account the purpose behind the DSARs. As regards to this, the Guidelines 01/2022 give clear guidance regarding the purpose of the submission of a DSAR which I have already mentioned above. Therefore, the case *Lees v Lloyds Bank Plc* EWHC 2249 (Ch) cannot influence the outcome of this Decision.

#### 5.4. Regarding previous similar complaints against the Controller:

5.4.1. Even if I accepted the Controller's position regarding their timely response to many requests submitted by the Law Firm, it cannot be ignored that, my Office had received two more complaints which were not submitted by the said law firm. The complaints had been lodged to the Austria and Malta SAs and thereafter received by my Office and referred to the Controller's failure to respond to two access requests.

5.4.2. Regarding the first complaint, I was of the view that the mere delay appeared to be a minor infringement which had only slightly affected the data subject's rights and freedoms. Therefore, I considered that the investigation proceedings could be concluded as no further supervisory measure was necessary at that stage. I informed the Controller about the conclusion of the case, on 05/01/2023.

5.4.3. Regarding the second complaint, considering both the moderating and aggravating factors, I decided, on 23/10/23, to issue a reprimand to the Controller to ensure that in the future they handle the data subject rights in accordance with the provisions of the Article 12(3). I also mentioned that, in case of a similar incident, that would be handled more strictly and the present complaint would be taken into consideration on taking any supervisory measures.

#### **6. Conclusion**

6.1. Having regard to all the above information, and based on the powers vested in me by Articles 58 and 83 of the GDPR, I conclude that there is an infringement by Brivio Limited, of Article 12(3) of the GDPR, for the reasons mentioned above.

6.2. Moreover, following an infringement of Article 12(3), as explained above, under the provisions of Article 83 of the GDPR, I take into account the following mitigating (1-3) and aggravating (4-7) factors:

1. The Controller fulfilled the Complainant's DSAR shortly after being informed that a complaint was lodged with my Office.
2. The measures taken by the Controller after the incident to ensure that staff properly fulfils their professional duties and supervise the correspondence management process.
3. The Controller's cooperation with the supervisory authority.
4. The Complainant's DSAR was not satisfied within the legal timeframe.
5. The lack of appropriate measures for dealing with data subject requests to exercise their rights, in a timely manner.
6. The Controller only became aware of the DSAR after being notified of the complaint by my Office.
7. The two relevant previous infringements by the Controller, of the GDPR.

6.3. In view of the above and on the basis of the powers conferred on me by the provisions of subparagraph (i) of paragraph (2) of Article 58 of the GDPR, **I have decided to impose an administrative fine of €2,000 (two thousand euro) pursuant to Article 83, to Brivio Limited for the infringement of Article 12(3) of the GDPR.**

Irene Loizidou Nicolaidou  
Commissioner  
For Personal Data Protection