Information and Data Protection Commissioner

CDP/COMP/344/2022

[redacted]

vs

[redacted]

COMPLAINT

1. On the 25th August 2022, [redacted], through her legal counsel (the **"complainant"** or the **"data subject"**) lodged a complaint with the Information and Data Protection Commissioner (the **"Commissioner"**) pursuant to article 77(1) of the General Data Protection Regulation[1] (the **"Regulation"** or the **"GDPR"**), alleging that the [redacted] (the [redacted]) has multiple data protection shortcomings, which the complainant *"identified from the date on which [redacted] first requested access to her son's file from the [redacted] this being on 24 May 2022, till the day of collection, this being 30 June 2022"*. Therefore, the complainant considered that the [redacted] infringed the data protection rights of her minor son.

FACTS OF THE CASE

2. For the purpose of this complaint, the Commissioner assessed the relevant facts surrounding the complaint:

   Summary of Events

   a. that the complainant alleged that the data protection rights of her minor son, including her rights as a parent, have been infringed by the controller when she submitted a request with the [redacted] to access the personal data of her minor son;

   b. that the complainant's son used to attend school at [redacted] ("[redacted]") in Pembroke where the [redacted] provides its services through therapists,

[1] 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.

including speech therapists and occupational therapists, to aid the children's better development and progress;

c. that as part of the curriculum, the therapists conduct an assessment at the beginning of each scholastic year where they assess every child and set individual goals for the year ahead and subsequently, the therapists continue seeing the children at [redacted] throughout the scholastic year;

d. that at the end of each scholastic year, the goals set at the beginning of the year are reviewed and the children are assessed again to determine which goals have been reached and which haven't, following which the therapists proceed to collect their conclusions in a report. The complainant explained that such assessments and report would then be placed in the child's file;

e. that, on the 24th May 2022, the complainant submitted a request by means of an email to the occupational therapist and the speech therapist who both work at the [redacted] and are the specialists who followed the complainant's son for the past scholastic year at [redacted];

f. that by means of an email dated the 24th May 2022, the complainant requested access to her son's file, and more specifically *"a copy of all the information in [redacted]'s file regarding OT and speech"*, however the complainant argued that such request seemed to be completely ignored by the therapists as neither a reply on this point, nor any direction whatsoever as to what the procedure for the obtainment of such file involves, was ever received;

g. that in view of such lack of provision of information, on the 10th June 2022, the complainant then sent an email to the [redacted] Director, to enquire when will she be provided with the requested file. The Director replied back three (3) days later, on the 13th June 2022, wherein she informed the complainant that she will be preparing a copy of the file for her to pick up. When the complainant emailed [redacted] Director again on the 15th June 2022 to request the file in anticipation of a meeting concerning the child which was due to happen the following day, the [redacted] Director replied back saying that her request was being *"processed according to GDPR procedures"*, but no information whatsoever was provided as to what such procedures entailed nor as to when the complainant should expect to have her son's file in hand as per her request. The complainant and the father of the minor, being unaware of what such procedures were supposed to consist of, kept pressing the [redacted] Director for the provision of such requested file. The [redacted] Director replied via email on the 17th June 2022 and informed the parents that they *"may wish to direct your queries on the matter to our data protection officer"*;

h. that on the 23rd June 2022, the [redacted] Director got in touch again by means of an email where she informed the complainant that she may view and collect the minor's file on the 27th June 2022 at 1pm from her office. Such appointment was then postponed by the [redacted] Director by thirty (30) minutes at which new time the complainant was unavailable due to school runs. Instead, the complainant offered to pass by the [redacted] Director's office the following day. The [redacted] Director replied that she will be unavailable on that day and further postponed the meeting to the 4th July 2022 at 12.30pm. The complainant in view of the stretch of time which had already passed since her original request on the 24th May 2022, and in view of requiring such files for meetings which she had scheduled with representatives from the minor's new school at which he will be attending from the next scholastic year, requested that she picks up her son's file on the 30th June 2022. To this, the [redacted] Director replied that the request for access was formally placed on the 10th June 2022. She further informed the complainant that she is the *"data controller for* [redacted] *and requests had to be received directly from yourself in writing and directly to me and not through any other route"*;

i. that a week prior to collecting the file from the [redacted] Director's office on the 30th June 2022, the complainant received a call from the Data Protection Officer (the **"DPO"**) of the [redacted] The DPO asked the complainant what it was that she required, and she explained that she had sent an email on the 24th May 2022 requesting visibility and access to her son's file. The DPO explained that there are certain data protection procedures which must be adhered to internally by the [redacted] before releasing such information. More specifically, the DPO mentioned that the go ahead for the release of such information following an access request rested solely in the DPO's hands. During such call, the DPO also mentioned that, in general, following the receipt of an access request, the [redacted] had to revert within thirty (30) days and if this is not possible, detailed reasons for such delay must be given;

Privacy Notice

j. that the complainant has taken into account all the data protection shortcomings which she has identified from the date on which the first request for access to her son's file was made (24th May 2022) till the day of collection (30th June 2022);

k. that throughout her contact and exchanges with the [redacted]'s representatives and employees, the complainant was never given, nor directed to, a privacy notice. When the complainant approached her legal counsel, her lawyer started looking for the [redacted]'s privacy notice, however, this proved to be very difficult to locate even for *"legal professionals holding qualifications in data protection"* let alone for a data subject;

l. that to locate the [redacted] privacy notice, the legal counsel first went onto the [redacted] 's website[2], but there was no privacy policy available on the website's home page. The complainant's legal counsel clicked on the drop-down menu under [redacted] ', selected [redacted], which led to a page about the [redacted], providing general information, yet reference to the [redacted] ' privacy notice was nowhere to be found. When attempting to do a general search on Google for [redacted] *Malta'* and clicking on the second option '[redacted]', this led the lawyer to a page with a notice marked in bold capital font in red reading: *'PAGE IS CURRENTLY UNDER CONSTRUCTION!'*. Following this, the complainant's counsel did another general Google search where we typed '[redacted] *data protection notice Malta'* and the first result which came up was the *'Data Protection Policy'* of the [redacted];

m. that after reading through the [redacted] 's *'Data Protection Policy'*, a number of shortcomings were identified and which unfortunately, leave the data subject unclear as to the main information that a privacy notice should provide transparency on, and this as outlined in article 13, article 14 and article 15 of the Regulation;

n. that from the [redacted] 's *'Data Protection Policy'*, the complainant outlined various shortcomings that have been identified as being in breach of the requirements under the Regulation as well as of the standards established by the European Authorities, including the European Data Protection Board (**"EDBP"**) in its numerous guidelines issued since the coming into force of the Regulation in 2018, in particular *'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default'*[3] (**"Guidelines 4/2019"**);

i. Confusion as to the identity of the Controller

o. that the *'Data Protection Policy'* appears to list the [redacted] Director, as the *'Data Controller'* which seems to be an incorrect designation of the identity of the data controller here. In the complainant's view, the Director is simply an employee within the [redacted], and it is the [redacted] which controls the children's personal data and which, from the same *'Data Protection Policy'*, seems to determine the purposes and the means of the processing of such data;

p. that in addition to the above, the *'Data Protection Policy'* makes reference the Processing of Personal Data (Education Sector) Regulations, (**"Subsidiary Legislation 586.07"**), wherein

[2] https://education.gov.mt/en/Pages/educ.aspx#
[3] European Data Protection Board, *'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default'*. Version 2.0 adopted on the 20th October 2020.

a controller is defined as *'education authorities, education institutions, examination bodies and the Corporation'*. When referring to the definition of *'education authorities'* in the same Subsidiary Legislation 586.07, these regulations cross-refer to Part II of the Education Act, which Part II, however, seems to have been repealed by Legal Notice 373 of 2021. This, **therefore, leaves a lacuna in the law and no proper definition as to what the** *'education authorities'* **referred to in SL 586.07 actually consist of;**

q. that the [redacted] may possibly be identified as an ***'education institution'*** within the meaning of Subsidiary Legislation 586.07, since it offers ***'Educational Psycho-social Services'*** as well as ***'Inclusive Education Support'***[4], and therefore would fall within the definition of a data controller within the meaning of Subsidiary Legislation 586.07.

r. that in line with the above considerations, the complainant believes that the [redacted] should be considered as the controller, and this to the exclusion of any other individual or employee within the same organisation. In this sense, the ***'Data Protection Policy'***, as well as the information being handed out by the [redacted] about itself and the identity of the controller, appear to be incorrect and misleading;

ii. Lack of clarity on the categories of personal data concerned and the identity of the data subjects

s. that the *'Data Protection Policy'* does not list the categories of data collected by the [redacted] The complainant further added that it also does not mention whether any special category data is collected and, or processed, nor does it outline any lawful bases under article 6 of the Regulation or conditions for processing under article 9 of the Regulation. However, it may be inferred that the [redacted] does in fact collect and, or process special category data, particularly, but possibly not solely, health data of the children to whom it provides support services, which children generally suffer from special conditions, such as down syndrome. As a result, the *'Data Protection Policy'* fails to provide the specific, explicit and legitimate purposes as to why such data is being collected;

t. that the *'Data Protection Policy'* does not provide any indication on how data is collected and from whom. There is also no indication as to the identity of the data subjects, except reference to children who are still not identified as ***'data subjects'***. It is also unclear whether the children's guardians, are or may be the data subjects of the [redacted] The complainant questions how individuals can know what rights they have vis-à-vis the [redacted] if there is no

[4] [redacted]

certainty whether such person is in fact a data subject of the same organisation. There is also no mention as to the interplay between children and their guardians in the sense that it is unclear from the *'Data Protection Policy'* whether the guardians of such children may exercise rights on behalf of their minor children and if so, to what extent and in what manner. Unfortunately, this lack of transparency is reflected throughout all sections within the *'Data Protection Policy'*;

iii. Lack of clarity on the purposes of data collection and processing, and legal bases for the same

u. that the *'Data Protection Policy'* includes a vague one-liner stating that, *"[t]he [redacted] collects and processes information to carry out its obligations in accordance with present legislation"*. The complainant argued that this is not sufficient and not in compliance with the Regulation since it lacks transparency and clarity about the purpose/s why the data are collected and processed by the [redacted];

v. that with reference to the legal bases for processing, there is no proper explanation of the obligations to which the [redacted] is referring and using as a basis for the collection and processing of children's personal data. The complainant noted that reference is made to *'present legislation'*, without any context whatsoever, and therefore she believes that this is also vague and certainly, insufficient;

iv. Lack of clarity on who the recipients/categories of recipients of the personal data are

w. that the *'Data Protection Policy'* does not specify the recipients or categories of recipients of the personal data being processed. It simply provides, in a very general manner, that *"[p]ersonal data will be disclosed to a number of data processors who provide the various services on behalf of the [redacted] and any relevant Health Authorities"*, as well as to *"third parties but only as authorised by law"*. The *'Data Protection Policy'* falls short of providing a clear and direct indication of whom these *'data processors'*, including the relevant *'Health Authorities'* and other *'third parties'* are. As outlined in Guidelines 4/2019[5], *"[t]he controller must be clear and open with the data subject about how they will collect, use and share personal data. Transparency is about enabling data subjects to understand, and if necessary, make use of their rights in Articles 15 to 22"*. The result of all this lack of clarity and lack of transparency is that the data subject, or as in this case, the persons acting on behalf of the minor, is left pondering as to the reasons why personal data are collected, processed and

[5] Ibid 3

shared by the organisation, and this makes it even more difficult for the data subject to exercise his or her rights in terms of the Regulation;

v. Lack of clarity on Data Subjects' Rights

x. that in line with the above observations, in particular, and with reference to the right of access, the *'Data Protection Policy'* provides that access requests are to be sent directly *"to the Director of the* [redacted]", and the complainant believes that since the organisation has a DPO, such requests should be sent to the [redacted]'s DPO, and not to its Director;

y. that the *'Data Protection Policy'* does not provide substantive information on the other rights pertaining to the data subjects *"rectification, erasure, restriction, objection, and data portability"* in relation to the use of their personal data by the [redacted]. It also does not provide information as to how the data subjects are to exercise any of such other rights. In addition to all this, the complainant noted that whilst personal data may be collected on the basis of consent, nowhere in the *'Data Protection Policy'* or in the provided consent form, is explained that the data subjects shall have the right to withdraw their consent at any time or how they may do this;

vi. No access to data retention policy

z. that the *'Data Protection Policy'* generally provides that *"retention requirements for the data processed within the* [redacted] *are outlined in the specific retention policies"* and that data *"that needs to be destroyed after the noted timeframes will be disposed of in an efficient manner"*. However, the *'Data Protection Policy'* contains no link or links as to what these retention policies are or from where these can be accessed by the data subjects. There is also no indication as to the criteria used to determine any such *'noted timeframes'* of the data being processed. The *'Data Protection Policy'* does not provide any information whatsoever as to the duration of the storage of personal data;

aa. that all this further contributes to the lack of transparency regarding the gathering and use of personal data of data subjects, the majority of whom are vulnerable individuals, children with special needs requiring the educational support services provided by the [redacted];

No internal data protection procedures & no reason or justification provided for delay

bb. that whilst both the Director as well as the [redacted]'s DPO mentioned *'GDPR procedures'* which need to be adhered to prior to documentation being provided following an access request, no proper explanation was ever given to the complainant as to what such GDPR procedures entailed. Neither was she contacted by the [redacted] after submitting her request with the therapists employed by the [redacted] on the 24th May 2022, and thus, it is clear that the **complainant**'s request was initially mishandled and ignored;

cc. that the complainant was left in the dark and this until she contacted the [redacted] Director, directly on the 10th June 2022 from when, not only such GDPR procedures were still never not explained to her, but her request continued being delayed without justification or reasons given. The [redacted] Director's email of the 30th June 2022, wherein she stated that the **complainant**'s request was *'formally'* made on the 10th June 2022 with her as the controller, could most certainly not be considered as a justification for such delay. This is also since the **complainant**'s access request was actually, and formally, made on the 24th May 2022 with the [redacted] therapists. It was then up to such employees to be informed and aware of the internal procedures within the [redacted] which are to be adhered to when receiving a data subject access request, including how to handle such request and whom to direct it to. In this regard, the complainant referred to the *'Guidelines 01/2022 on data subject rights - Right of access'*[6] (the "**Guidelines 01/2022**"), which provide that, *"[t]here are no specific requirements on the format of a request. The controller should provide appropriate and user-friendly communication channels that can easily be used by the data subject. However, the data subject is not required to use these specific channels and may instead send the request to an official contact point of the controller"*;

dd. that more than thirty (30) days passed from when the complainant submitted her request with the [redacted] on the 24th May 2022, until she collected her son's file on the 30th June 2022, and no reasons or explanations were ever given to her for such delay and this even though such request was most certainly not 'complex' within the meaning of the Regulation;

ee. that the inconsistencies with which the complainant was faced when communicating with the [redacted] representatives lead one to think that, in reality, no such formal GDPR procedures actually exist within the [redacted]. This is, in particular, being stated as the DPO had told the complainant that it was she who gave the go ahead for the release of personal data following

[6] European Data Protection Board, *'Guidelines 01/2022 on data subject rights - Right of access'*, Version 1.0, adopted on the 28th March 2023.

an access request, the [redacted] Director had given a completely opposite impression when, in her email dated the 30th June 2022, she had specifically informed the complainant that access requests had to be directed directly to her and *'not through any other route'*;

ff. that the way in which the complainant's access request was handled, provides a clear indication that there is a lack of internal awareness across the board within the [redacted] as to the GDPR obligations applying to the [redacted] as the controller.

Access was not facilitated

gg. that the lack of clarity and transparency on data subjects' rights under the *'Data Protection Policy'*, as explained further above, as well as the manner in which the complainant made the request via email but was requested to go pick up the file in person, certainly did not facilitate access to the personal data of her son. This also contrary to article 12 of the Regulation where it is specifically provided that if *"the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject"*. It may, therefore, be clearly inferred that the [redacted] does not employ any safe encrypted transmission methods, or if it does employ them, they were, for some reason or another, not resorted to in this case;

hh. that the [redacted] Director further delayed pick up of the requested file by two (2) days, and if it were not for the complainant's insistence, [redacted] would have further delayed pick up till the 4th July 2022;

ii. that contrary to the controller's obligation under the Regulation to facilitate the exercise of the data subjects' rights, in this case, exercise of the right of access, or of any other right granted under the Regulation for that matter, is not at all rendered easy for the data subject.

INVESTIGATION

Request for submissions

3. Pursuant to article 58(1)(a) of the Regulation, the Commissioner provided the [redacted] with a copy of the complaint, including the documentation attached thereto, and requested it to put forward its submissions in order to defend itself against the allegations raised by the complainant. By means of an email dated the 3rd October 2022, the [redacted] submitted the following principal arguments for the Commissioner to consider in the legal analysis of the case:

a. that the [redacted] therapists keep seeing the children at [redacted] throughout the scholastic year according to their individual needs, whilst all assessments, reports and observations are placed in each child's file. The [redacted] noted that it is a fact, and it is unjust that the complainant seems to imply that the assessments and reports are *'supposedly'* placed in the child's file. Furthermore, it was alleged that the right of access request was submitted on the 24th May 2022 by means of an email sent to the occupational therapist and the speech therapist. The [redacted] argued that this is not entirely correct, as on the 24th May 2022, the complainant sent the email to the [redacted]'s Head of School and not to the occupational therapist and the speech therapist, and it was then that the Head of School who forwarded the email to the occupational therapist and the speech therapist, and copied in the complainant;

b. that unlike the allegation put forward by the complainant, the complainant's requests were definitely not ignored. Both therapists were replying to her emails and invited her to attend the professionals' meeting scheduled for the 16th of June 2022 at [redacted] Offices in Hamrun. During this meeting there would have been a professionals' handover between the therapists of [redacted] and [redacted], and the reports contained in the minor's file would have been discussed and explained in detail to the complainant. Normally, the only persons attending these handover meetings are the therapists from both schools, however the [redacted] had no objections for the complainant to attend this meeting, in line with her own request;

c. that, on the 9th of June 2022, the complainant demanded that other practitioners (from [redacted] to [redacted], within [redacted] and therefore not [redacted]) would be present for the professionals' handover meeting, and such a demand is not in line with the scope of this meeting since the practitioners were neither [redacted] nor [redacted] therapists nor even employees. Due to this and also due to the fact that a similar meeting with the same practitioners was scheduled at the [redacted] on the same day (16th June 2022) for which both the complainant and the same [redacted] practitioners of her choice were going to be present, on the 9th of June 2022, the [redacted] Director sent an email to her to inform her that former professionals' handover meeting was being cancelled;

d. that the [redacted] Director's reply to the complainant, three (3) days after receiving the email, is in line with [redacted] and on the 10th June 2022, the complainant requested only the speech therapy file and then further requested the occupational therapy file on the 13th of June 2022. Therefore, on the 13th of June 2022, the [redacted] Director replied that she will be providing both files as requested;

e. that during such transition meetings, parents never have their child's file in hand;

f. that following the [redacted] Director's reply to the complainant dated the 13th June 2022 where she clearly stated that she would be preparing the requested files, and the subsequent reply from the [redacted] Director to the complainant dated the 15th June 2022, informing her that such requests have to be processed according to the GDPR procedures and that her request was being processed, both the complainant and her partner argued that as parents of the minor, they did not need to go through GDPR procedures to access such files leading the [redacted] Director to understand that they were both aware of such GDPR procedures even because at no point did they question her to explain what such procedures consist of. However, following this exchange, in an email dated the 17th June 2022, the [redacted] Director rightly directed them to [redacted] DPO who could explain in detail such procedures. In the same email, the [redacted] Director offered the minor's parents to schedule a meeting where they could view the original copies of the file (following their allegations that the requested files did not really exist);

g. that the complainant never replied to the email to confirm the appointment given by the [redacted] Director on the 27th June 2022 at 1pm, to collect the files. However, on the 26th June 2022, the [redacted] Director informed the complainant that the appointment had to be postponed by just thirty (30) minutes due to unforeseen circumstances. It was only on the 27th June 2022 that the complainant informed the [redacted] Director that she is always available to pick up the files until 11:30am latest. This means that prior to this communication, the [redacted] could have never been in a position to provide her with an appointment which suited the complainant's needs since she was not aware of these time constraints. Furthermore, up to this point, the agreement between the [redacted] Director and the complainant was that the files are personally handed by the [redacted] Director during an appointment where she would go through the files and explain any technicalities (in line with the controller's obligation to not simply hand the data but explain it to the data subject as and where necessary). By means of an email dated 27th June 2022, the complainant informed the [redacted] Director to leave the files with the receptionist in a sealed envelope, meaning that she no longer requested to be given any explanation of technicalities and was only interested in obtaining a copy of the files;

h. that none of the minor's parents ever sent the DPO an email. On the 17th June 2022, the DPO had received instructions from the [redacted] to call the complainant. The DPO called her immediately on the next business and during this phone call, the DPO asked the complainant to explain to her the issue. Thus, the DPO explained to her that as per the Regulation, she indeed has the right to access all the personal data that the [redacted] keeps and processes about her son;

i. that it is untrue that the complainant encountered inconsistencies between the [redacted] Director and the DPO. The [redacted] noted that at no point in time did the DPO tell the complainant that it is the DPO's role to give the go ahead to a controller to give the information requested to the data subject;

j. that the original request made on the 24th May 2022 was amended on various instances where she kept asking for more files and reports. Thus, the actual material given to her on the 30th June 2022 was even more than what she originally requested on the 24th May 2022;

k. that regarding the allegation that no privacy policy is available on the [redacted]'s website, the [redacted] noted that this is not correct, as on the [redacted] website, a generic *'Data Protection Policy'* for [redacted] was uploaded on the 26th April and this is easily accessible under the tab [redacted] in which menu there is an entry *'Data Protection'*. The [redacted]'s *'Data Protection Policy'* is found on the [redacted] website, tab *'Useful Links'* and in its menu, there is the second option entitled *'Data Protection Policy'*;

l. that regarding the arguments raised by the complainant in relation to the *"Confusion as to the identity of the Controller"*, the [redacted] noted that whenever a [redacted] designates a new controller or undergoes a change in the person acting as controller, the [redacted] informs the [redacted] in writing. Since this is a generic *'Data Protection Policy'* for [redacted] it states: *"Your personal data is collected under one of the legal grounds outlined in Article 6 of the GDPR, depending on the service being provided"*. The [redacted] then has other Data Protection Policies for specific services, thus the allegation that the *'Data Protection Policy'* does not outline any lawful bases under article 6 of the Regulation is unfounded;

m. that regarding the arguments raised by the complainant in relation to the *"Lack of clarity on the purposes of data collection and processing, and legal bases for the same"*, the [redacted] stressed that this is a generic *'Data Protection Policy'* for all [redacted] What the complainant failed to mention was that in this policy there is also written that *"[t]he [redacted] strives to enhance the holistic development of ALL children [redacted] provides equitable and high-quality services focusing on the physical, social, emotional, psychological, cultural, and behavioural development of children within an inclusive-oriented culture, aimed at eliminating challenges and barriers, to help children reach their full potential"*;

n. that regarding the arguments raised by the complainant in relation to the *"Lack of clarity on the categories of personal data concerned and the identity of the data subjects"*, the [redacted]

outlined that it uses the intranet templates and fill in details where requested by the template and follow the procedure as explained;

o. that regarding the arguments raised by the complainant in relation to the *"Lack of clarity on Data Subjects' Rights"*, the [redacted] noted that since the organisation has a DPO, such requests should be sent to the DPO of the [redacted], and not to its Director. Data subjects' requests for access are to be made to the controller and not the DPO, and this is also pre-written in the *'Data Protection Policy'* template;

p. that the [redacted] made reference to the complaint, specifically to the argument that *"[n]owhere in the Policy or in the provided consent form, is there explained that the data subject shall have the right to withdraw **their consent**"*. The [redacted] noted that it is working together with the DPO to review all consent forms to ensure compliance with the Regulation. The exercise was finalised in time for the start of the new scholastic year (2022-2023);

q. that with respect to the *'Retention Policy'*, the [redacted] has been working on its retention policy and the exercise has almost been finalised and the policy shall be uploaded on the [redacted] website in the coming days;

r. that even if the 24th May 2022 is to be taken as the original date of the full request, the [redacted] was still within the established timeframes by article 12(3) of the Regulation as the [redacted] Director sent the email to the complainant on the 23rd June 2022, and the file was therefore accessible to the complainant in line with her original request and also her added requests well within the timeframes established by the Regulation;

s. that the personal files of students held with the [redacted] contain very sensitive information regarding specific health issues and conditions. It is because of this that the DPO had suggested that copy of the file should not be sent by email but rather collected by hand by the complainant or a person officially designated by her. The [redacted] further noted that when sending an email one can never be sure whether that email account is in reality being accessed by any third parties and thus, is not a question of encryption; and

t. that the [redacted] proceeded with utmost caution in the said case as it does with its everyday practices and also adhered to the GDPR obligations, whilst bearing in mind the sensitive nature of information which it holds.

4. On the 7th October 2022, the Commissioner provided the complainant with the opportunity to rebut the arguments made by the [redacted] On the 17th October 2022, the complainant noted that she has no further submissions to make on the matter. Following this, and in line with the Office's complaint-

handling procedure, the Commissioner provided the controller with the final opportunity to put forward additional arguments and, in this regard, on the 19th October 2022, the [redacted] submitted that the submissions provided on the 3rd October 2022 were indeed final.

5. On the 16th February 2023, the Commissioner requested the [redacted] to provide further clarifications and documentation to take into consideration during the legal analysis of the case. Particularly, (i) "*to clarify whether the incomplete policies mentioned in your submissions are finalised or otherwise, and if in the affirmative, you are hereby being requested to provide a copy of these policies; (ii) to provide a copy of the data protection policies mentioned in the* [redacted] *submissions, wherein it was stated that* [redacted] *' then has other DP Policies for specific services*"; *and (iii) to provide the necessary clarifications of who manages the personal data of minors utilising the* [redacted] *services, specifically who is responsible for the processing of such personal data*". In this regard, by means of an email dated the 1st March 2023, the [redacted] provided a copy of the complete retention policy entitled *'Policy Regulating Retention of Documentation in* [redacted] *)'*, which was finalised and published on the [redacted] ' website[7] on the 10th November 2022. Additionally, the [redacted] provided a copy of the finalised [redacted] and, re-confirmed that the *'* [redacted] *Director is the Data Controller of* [redacted] *and as such determines the purposes and means of data processing within the Department*".

LEGAL ANALYSIS AND DECISION

The identity of the controller

6. As a preliminary step of this legal analysis, the Commissioner sought, in essence, to establish whether the [redacted] or the [redacted] Director is acting in its role of the controller in relation to the processing of the personal data of minors using the [redacted] services.

7. Accordingly, the Commissioner examined article 4(7) of the Regulation, which defines the term controller as "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*".

[redacted]

8. In this regard, the Commissioner analysed the accountability principle enshrined in article 5(2) of the Regulation, which provides that the controller shall be responsible for, and be able to demonstrate compliance with the principles relating to the processing of personal data as set out in article 5(1) of the Regulation. This principle of accountability stipulates an overarching compliance with the aim and purposes of the Regulation, which is essential to safeguard the rights and freedoms of the data subjects. It therefore follows that the controller is the main entity bound by the provisions of the Regulation and has responsibility and liability in terms of compliance.

9. The crucial aspect for assuming the role of a controller is the determination of the *"means"* and the *"purposes"* of the processing. In other words, the controller should decide, in an autonomous manner, certain key elements about the processing and consequently, exercise decisive influence over the same processing activity. **Indeed, the Court of Justice of the European Union ("CJEU") in** its settled jurisprudence[8] interpreted the concept of controller in a pragmatic and functional fashion as averse to a purely formal analysis. In doing so, the CJEU examined thoroughly the factual influence that actors had over the respective processing activities.

10. In this regard, in its *'Guidelines 07/2020 on the concepts of controller and processor in the GDPR'*[9] (the **"Guidelines 07/2020"**), the EDPB stressed that *"the concept of controller is a functional concept, it is therefore based on a factual rather than a formal analysis"* and *"it may be that the formal appointment does not reflect the reality of the arrangements, by formally entrusting the role of controller to an entity which actually is not in the position to "determine" the purposes and means of the processing"*.

11. Another essential component of the definition of *"controller"* is the object of control, which refers to the purposes and means of the processing, which is loosely translated into the *"why"* and *"how"* of the processing operation. From a purely terminological perspective, *"purpose"* is defined as the *"anticipated outcome that is intended or that guides your planned action"*, and the *"means"* is *"how a result is obtained or / and is achieved"*. In this context, the Regulation states that personal data shall be collected for specified, explicit and legitimate purposes and that, as a general rule, it shall not be further processed in a manner that is incompatible with those purposes.

12. In the analysis of the current case, the [redacted] reiterated in its submissions that *'[redacted] **Director is the Data Controller of** [redacted] and as such determines the purposes and means of data processing*

[8] Judgement of the Court (Grand Chamber) of the 13th May 2014, *'Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González'*, C-131/12, ECLI:EU:C:2014:317; and Judgement of the Court (Grand Chamber) of the 5th June 2018, *'Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH'*, C-210/16, ECLI:EU:C:2018:388.
[9] European Data Protection Board, *'Guidelines 07/2020 on the concepts of controller and processor in the GDPR'*, Version 2.1 adopted on the 7th July 2021.

within the Department". For this purpose, the Commissioner proceeded to conduct an exercise to determine, whether the [redacted] Director fulfils the role of a controller, and proceeded to assess the Guidelines 07/2020[10], outlining that *"[s]ometimes, companies and public bodies appoint a specific person responsible for the implementation of the processing activity.* ***Even if a specific natural person is appointed to ensure compliance with data protection rules, this person will not be the controller but will act on behalf of the legal entity*** *(company or public body) which will be ultimately responsible in case of infringement of the rules in its capacity as controller"* [emphasis has been added].

13. After carefully consideration of the Guidelines 07/2020[11], the Commissioner has concluded that the controller in question is the [redacted], and not the [redacted] Director, who is an employee of the Department.

The email sent to the [redacted] to exercise her right pursuant to article 15 of the Regulation

14. The Commissioner established that, on the 24th May 2022, the complainant sent an email to the [redacted]'s occupational therapist, whilst keeping in copy the [redacted]'s speech therapist, [redacted]'s Head of School and another member of the [redacted] staff, wherein she requested the [redacted] to provide *"a copy of all the information in* [the minor's] *file regarding OT and speech"* **(annexed and marked as Doc. IDPC 1)**.

15. From the initial contents of the complaint and the controller's submissions, the Commissioner established that on the 10th June 2022, the complainant sent an email to the [redacted] Director enquiring when the information requested will be available. The [redacted] Director replied three (3) days later, stating that the documentation requested is being prepared and she will be contacted accordingly to collect it. By means of an email dated the 15th June 2022, the complainant communicated with the [redacted] Director and stated that *"I need the reports by today as meeting will be held tomorrow"*. The [redacted] Director replied on the same day by saying that *"such requirements have to be processed according to GDPR procedures. To this effect your requirement is being processed"*. In this regard, the Commissioner analysed the reply provided by the [redacted] Director on the 29th June 2022, outlining that *"[a]s you are well aware* ***you made your formal request on the 10th June to myself as the data controller****, which means that contrary to your claim I am still within the limits"* [emphasis has been added] **(annexed and marked as Doc. IDPC 2)**.

[10] Ibid 9.
[11] Ibid 9.

16. The Commissioner assessed Guidelines 01/2022[12], wherein the EDPB outlined that *"[t]he controller is also not obliged to act on a request sent to the e-mail address of a controller's employee who may not be involved in the processing of requests concerning data subjects' rights (e.g. drivers, cleaning staff, etc.). Such requests shall not be considered effective, if the controller has clearly provided the data subject with appropriate communication channel.* ***However, if the data subject sends a request to the controller's employee who has been assigned to them as their regular contact person*** *(such as e.g. a personal account manager at a bank or a regular consultant at a mobile phone operator),* ***such contact should not be considered as a random one and the controller should make all reasonable efforts, to handle such a request so that it can be redirected to the contact point and answered within the time limits provided for by the GDPR"*** [emphasis has been added].

17. The Commissioner referred to the email sent by the [redacted] Director on the 29th June 2022, stating that *"[a]s you are well aware* ***you made your formal request on the 10th June to myself as the data controller, which means that contrary to your claim I am still within the limits"*** [emphasis has been added]. In this regard, the Guidelines 01/2022[13] notes that the controller should make all reasonable efforts so that any requests made through the generic email address are redirected to the data protection contact point and answered within the time limits provided for by the GDPR. Moreover, ***"the controller is not entitled to extend the period for responding to a request, merely because the data subject has sent a request to the controller's general e-mail address, not the controller's data protection contact point e-mail address"*** [emphasis has been added].

18. In this respect, the Commissioner noted that even though the complainant did not submit the subject access request to the email address provided on the [redacted] *'Data Protection Policy'* available on its website, but rather exercised her right by means of an email sent to the [redacted]'s Therapists, it is still considered to be an effective request, as it was submitted to employees who dealt with the complainant's minor's affairs on a daily basis. Therefore, the Commissioner established that the date when the complainant exercised the right to access personal data on behalf of her minor son with the [redacted] was indeed the 24th May 2022.

The Complainant's Subject Access Request

19. Within this context, the Commissioner examined article 15 of the Regulation which gives the data subjects, 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

[12] Ibid 6.
[13] Ibid 6.

and to the information listed in article 15(1) of the Regulation. Furthermore, the controller has the obligation to provide the data subject with a copy of all the personal data pertaining to the data subject undergoing processing, without affecting the rights and freedoms of others.

20. Having considered that the right to access one's own data is not only acknowledged under article 15 of the Regulation, but it is also set out as an element of the fundamental right to the protection of personal data, recognised by article 8(1) of the Charter of Fundamental Rights of the European Union[14]. Within this context, the rights of the data subjects as laid down in articles 12 to 22 of the Regulation, are the fulcrum and the basis of the law, and their role is crucial to ensure effective and comprehensive protection of the personal data processed by controllers.

21. Having noted the importance attributed to the right of access as a component of the fundamental right to data protection as enshrined in the Charter, particularly article 8(2) which specifically provides that everyone has the right of access to data which has been collected by the controller. Additionally, the right of access is framed within the objectives of data protection law and more specifically, the protection of *"fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data"*, as articulated by article 1(2) of the Regulation.

22. Having considered the right's fundamental role to ensure transparency and facilitate control, its specific inclusion in the Charter, and its historical significance, the right to access one's own personal data is part of the essence of the right to the protection of personal data, and any measure tempering with the existence of the right of access touches the very essence of the protection which both the Charter and the Regulation seek to achieve.

23. Having considered the ruling of the CJEU which stated that "*Article 12(a) of Directive 95/46 and Article 8(2) of the Charter of Fundamental Rights of the European Union must be interpreted as meaning that an applicant for a residence permit has a right of access to all personal data concerning him which are processed by the national administrative authorities within the meaning of Article 2(b) of that directive. For that right to be complied with,* ***it is sufficient that the applicant be in possession of a full summary of those data in an intelligible form, that is to say a form which allows that applicant to become aware of those data and to check that they are accurate and processed in compliance with that directive, so that he may, where relevant, exercise the rights conferred on him by that directive***"[15] [emphasis has been added].

[14] Charter of Fundamental Rights of The European Union, 2012/C 326/02, published in the Official Journal of the European Union C 326/391 of 26th October 2012.
[15] CJEU, Joined Cases C-141/12 and C-372/12, ECLI:EU:C:2014:2081, rule n. 2.

24. In particular this right's special feature is derived from the fact that it is a mean, a prerequisite or a condition to enable data subjects to exercise control over their personal data, and consequently exercise other data subject rights, such as the right to erasure or rectification, as the case may be. The CJEU in the judgment *'Peter Nowak vs Data Protection Commissioner'*[16] held that *"it must be recalled that the protection of the fundamental right to respect for private life means, inter alia, that any individual may be certain that the personal data relating to him is correct and that it is processed in a lawful manner. As is apparent from recital 41 of Directive 95/46, it is in order to be in a position to carry out the necessary checks that the data subject has, under Article 12(a) of the directive, a right of access to the data relating to him which is being processed. That right of access is necessary, inter alia, to enable the data subject to obtain, depending on the circumstances, the rectification, erasure or blocking of his data by the data controller and consequently to exercise the right set out in Article 12(b) of that directive".*

25. The right of access as enshrined in article 15 of the Regulation contains (3) components: (i) confirmation of the processing of personal data; (ii) information about the processing itself, and (iii) access to a copy of the personal data undergoing processing.

26. Having assessed the wording of article 15(1) of the Regulation, which enables the data subject 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**"*, as well as other supplementary information pursuant to article 15(1)(a) to (h) of the Regulation. Further to this, article 15(3) of the Regulation, which is more prescriptive, states that *"**the controller shall provide a copy of the personal data undergoing processing**"* [emphasis has been added].

27. Having examined article 12(3) of the Regulation, which obliges the controller to *"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**"*, and recital 59 of the Regulation, setting out that *"[t]he controller should be obliged to respond to requests from the data subject without undue delay and **at the latest within one month** and to give reasons where the controller does not intend to comply with any such requests*" Additionally, article 12(3) of the Regulation stipulates that *"[t]he 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 request. 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** [...]"* [emphasis has been added].

[16] *'Peter Nowak vs Data Protection Commissioner'* (Case-434/16), decided on the 20th December 2017.

28. The Regulation provides the controller with the opportunity to extend the one-month deadline to comply with a request for access to personal data, but at the same time, it rules that the same controller informs the data subject of such extension, also indicating the reasons for the delay. In this case, while the initial date was considered, the [redacted]'s failure to provide the requested information within the one-month deadline, without an appropriate explanation or extension, is considered to be an infringement of the provisions of the Regulation.

29. In this connection, article 12 of the Regulation ensures that substantive rights of data subjects are safeguarded by establishing clear, proportionate and effective conditions as to how and when data subjects shall exercise their rights. In this regard, article 12 of the Regulation provides the modalities for **the exercise of the data subjects' rights and establishes an obligation upon the controller to** facilitate the exercise of these rights.

Access was not facilitated

30. Article 12(1) of the Regulation specifies that controllers must provide individuals with information regarding the processing of their personal data in writing, or by other means, including electronic means where appropriate. Furthermore, article 15(3) of the Regulation states that 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.

31. The Commissioner took into consideration the Guidelines 01/2022[17], stating that *"in some circumstances it could be appropriate for the controller to provide access through other ways than providing a copy. Such non-permanent modalities of access to the data could be, for example: oral information, inspection of files, onsite or remote access without possibility to download. These modalities may be appropriate ways of granting access for example in cases where it is in the interest of the data subject or the data subject asks for it".*

[redacted]'s *'Data Protection Policy'*

32. In her submissions, the complainant noted that the [redacted]'s *'Data Protection Policy'* was very difficult to locate, thus running contrary to article 12(1) of the Regulation. In order to sustain her claim, the complainant further added that *"we identified a number of shortcomings which, unfortunately, leave the data subject unclear as to the main information that a privacy policy should provide transparency on, and this a outlined in Article 13, 14 ad 15 of the GDPR".*

[17] Ibid 6.

33. During the course of the investigation, the Commissioner observed that the controller's website hosted on [redacted] (the "**website**").

34. One of the key principles of processing personal data is transparency, which is intrinsically linked to the principles of lawfulness and fairness. Altogether, this principle is laid down in article 5(1)(a) of the Regulation, which provision provides that personal data shall be *"**processed lawfully, fairly and in a transparent manner in relation to the data subject**"*.

35. The rationale behind the principle of transparency and the related provisions, particularly articles 13 and 14 of the Regulation, is that the data subject shall be made aware, *inter alia*, of the existence of the processing activity and be provided with certain essential information about the processing activity. In its Guidelines on Transparency under Regulation 2016/679[18], the Article 29 Working Party specified that transparency is an overarching obligation, which is necessary to enable data subjects to exercise their data protection rights in terms of articles 15 to 22 of the Regulation. In one if its judgments[19], the CJEU highlighted that the *"requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed, set out in Article 12 of Directive 95/46, and their right to object to the processing of those data, set out in Article 14 of that directive"*.

36. The Article 29 Working Party additionally provides that the *"**concept of transparency in the GDPR is user-centric rather than legalistic and is realised by way of specific practical requirements on data controllers and processors in a number of articles**. The practical (information) requirements are outlined in Articles 12 - 14 of the GDPR"*[20] [emphasis has been added]. The transparency principle is further articulated in recital 39 of the Regulation, which specifies that *"**it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.** The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used"* [emphasis has been added].

37. The Commissioner stresses that the controller should be held accountable in relation to the transparency of the processing of personal data, not only at the point of collection of personal data,

[18] Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679*, (17/EN, WP260 rev.01).
[19] Judgment of the Court (Third Chamber) of the 1st October 2015, *'Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others'*, (C-201/14, ECLI:EU:C:2015:638).
[20] Ibid 18.

but throughout the processing life cycle[21]. The Regulation explicitly articulates transparency as one of the principles of processing, which requires that personal data should be processed in a manner that is transparent to the data subjects. The principle of transparency is a fundamental condition for enabling data subjects to exercise control over their own personal data and to ensure effective protection of their personal data and exercise of their rights.

38. For this purpose, article 12(1) of the Regulation provides that the *"controller shall take appropriate measures to provide any information referred to in Articles 13 and 14... to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language"*. Furthermore, the Guidelines on Transparency under Regulation 2016/679 establish that the *"information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations. In particular the purposes of, and legal basis for, processing the personal data should be clear."* Therefore, in accordance with articles 13 and 14 of the Regulation, which stipulate that where personal data relating to a data subject are collected from the data subject and where personal data have not been obtained from the data subject, the controller should provide the data subject with certain information to ensure transparent processing. In fact, articles 13 and 14 of the Regulation provide for a predetermined set of elements that must be incorporated in the data protection policy, including *inter alia*, the contact details of the controller and where applicable, of the controller's representative, the contact details of the DPO *(if any)*, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing and the categories of personal data involved.

39. For the purpose, the Commissioner examined the WP29 Guidelines of Transparency under Regulation 2016/679[22], which stipulate that *"**[e]very organisation that maintains a website should publish a privacy statement/ notice on the website. A direct link to this privacy statement/ notice should be clearly visible on each page of this website under a commonly used term (such as "Privacy", "Privacy Policy" or "Data Protection Notice")**"*[23] [emphasis has been added].

40. Having considered article 13 and article 14 of the Regulation, which stipulate that where personal data relating to a data subject are collected from the data subject and where personal data have not been obtained from the data subject, the controller shall provide the data subject with certain information to ensure transparent processing.

---

[21] Ibid 18.
[22] 17/EN, WP 260 rev. 01, Section 11, Page 8. Example box: "*Every organisation that maintains a website should publish a privacy statement/ notice on the website. **A direct link to this privacy statement/ notice should be clearly visible on each page of this website under a commonly used term (such as "Privacy", "Privacy Policy" or "Data Protection Notice")***" [emphasis has been added].
[23] Ibid 18.

41. After examining the contents of the *'Data Protection Policy'* available on the [redacted]'s website[24], the Commissioner concludes that the Policy does not contain all the minimum information which shall be provided to the data subjects, pursuant to article 13 and article 14 of the Regulation.

[redacted]'s Internal Data Protection Policies

42. The Commissioner referred to the reply provided by the [redacted] on the 1st March 2023, when it submitted a copy of the complete retention policy entitled *'Policy Regulating Retention of Documentation in* [redacted]', which was finalised and published on the [redacted] website on the 10th November 2022, and the copy of the [redacted]

43. In his assessment, the Commissioner noted that the controller did not have in place any internal policies and processes to implement relevant data protection requirements for the particular processing operations carried out by the [redacted], which are binding on all employees handling personal data. These measures should be reflected in concrete practices and operationalised throughout the activities of the controller in order to reduce the risk of unauthorised access to personal data held by the controller. In fact, article 32(4) of the Regulation provides that the controller *"shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law"*.

44. Additionally, article 24(1) of the Regulation stipulates that, by virtue of the principle of accountability enshrined in the Regulation, the controller, taking into account the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with the same Regulation. This provision shall be read in combination with article 24(2) of the Regulation, which provides that *"[w]here proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of* ***appropriate data protection policies by the controller***" [emphasis has been added].

[redacted]

45. In one of its opinions[25], the WP29 stressed the importance of having such data protection policies in place, pointing out that certain measures that controllers may take to comply with the accountability principle *"[a]re 'staples' that will have to be implemented in most data processing operations.* ***Drafting internal policies and procedures implementing the principles".*** Accordingly, the controllers should not only ensure to have such policies in place, but also that such policies are aligned with the spirit and the scope of the Regulation. It is crucial for the controller to take active responsibility for ensuring compliance and develop an accountability culture at all levels of the department [emphasis has been added].

Training of employees

46. On the 12th September 2022, the Commissioner made a specific request to the [redacted] to confirm whether the employees in question had attended data protection training and to provide evidence of their attendance. However, when the [redacted] replied on the 3rd October 2022, the [redacted] only provided the training certificate of the [redacted] Director, which was obtained on the 1st June 2022. In his consideration, the Commissioner noted that not all employees in this particular case received the necessary training on data protection legislation despite being responsible for the handling of personal data, including special categories of personal data as part of her day-to-day duties.

47. The controller should ensure that all the employees handling personal data are provided with and are required to attend initial and ongoing data protection training in order to foster a culture of data protection and raise awareness among the employees about their responsibilities. This is also in line with article 39(1)(b) of the Regulation, which provides that the DPO shall provide training to personnel having permanent or regular access to personal data. The Article 29 Working Party[26] provides that "*the implementation of these measures and processes may also be done in an effective manner through the assignment of responsibilities and through the training of staff involved in the processing operations*".

48. The Commissioner outlined that the complainant's subject access request received on the 24th May 2022, sent by means of an email to an occupational therapist and a speech therapist, was not forwarded to the [redacted]' DPO to be dealt within the time-period stipulated by the Regulation. In this regard, the Commissioner proceeded to examine article 38(1) of the Regulation, which provides that "*[t]he controller and the processor shall ensure that* ***the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data***"

[25] Ibid.
[26] Article 29 Working Party, *'Opinion 3/2010 on the principle of accountability'* (00062/10/EN, WP 173), adopted on the 13th July 2010.

[emphasis has been added]. Such inherent principle of good governance was further developed by the Article 29 Working Party in the sense that "*[i]t is crucial that the DPO, or his/her team, is involved from the earliest stage possible in all issues relating to data protection*"[27]. The Belgian supervisory authority adopted the same approach in one of its decisions[28], whereby it underlined the crucial importance of consulting and not merely informing the DPO on matters relating to data protection in view of ensuring, *inter alia*, compliance with the law.

49. In this respect, the Commissioner examined the Guidelines 01/2022[29] outlining that "***the controller** should make all reasonable efforts, to handle such a request **so that it can be redirected to the contact point and answered within the time limits provided for by the GDPR**"* [emphasis has been added].

50. The Commissioner recognises the importance that all the employees handling personal data have the necessary data protection training to recognise when a SAR has been lodged, understanding the process for directing it to the DPO or designated contact point, and providing a response within the specified time frame. Therefore, the Commissioner stresses that comprehensive training on data protection is an essential tool to reduce delayed responses, missed deadlines, or even non-compliance with the Regulation. The controller should ensure that all the employees handling personal data are provided with and are required to attend initial and ongoing data protection training.

Exercise of corrective powers

51. Having scrutinised the set of corrective tools at the disposal of the Commissioner in its capacity of a supervisory authority pursuant to article 58(2) of the Regulation where the processing operation infringes the provisions of the Regulation, which include *inter alia* the power to impose an administrative fine pursuant to the general conditions laid down in article 83 of the Regulation.

52. The Commissioner therefore proceeded to examine article 83(2) of the Regulation, which provides certain guiding criteria in deciding whether to impose an administrative fine and on the amount of the administrative fine in each individual case. Having read such provision, the Commissioner established that these sub-paragraphs (a), (b), (f), (g) and (h) of article 83(2) of the Regulation are relevant to the present case.

---

[27] Article 29 Working Party, *'Guidelines on Data Protection Officers ('DPOs')*, (16/EN WP 243 rev. 01), endorsed by the European Data Protection Board.
[28] Decision APD/GBA - 18/2020 of the 28th April 2020 of the Litigation Chamber of the Belgian supervisory authority.
[29] Ibid 6.

Article 83(2)(a) of the Regulation

53. Due regard was given to article 83(2)(a) of the Regulation, which refers to "*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*".

54. The Commissioner examined the nature of the infringement, which relates specifically to the obligations of the controller as laid down in the Regulation. The Data Protection Act (Cap. 586 of the Laws of Malta) (the **"Act"**) sets up two different maximum amounts of administrative fines for public bodies and authorities, which indicate that an infringement of certain provisions of the Regulation may be more serious than other provisions. An infringement committed by the controller in relation to its obligations falls into the category of *"**a fine shall not exceed** fifty thousand euro (€50,000) for each violation and, additionally, the Commissioner may impose a daily fine payment of fifth euro (€50) for each day during which such violation persists*".

55. It is indeed the intention of the legislator to sanction any infringement of the data subjects' rights in a severe manner, considering that such rights are fundamental instruments at the disposal of the data subjects, which enable them to exercise control over their personal data within a stipulated time-frame. Thus, whilst assessing the gravity of the infringement, the Commissioner has also taken into account that the negligent behavior of the controller hindered the complainant from exercising a fundamental right within the period stipulated by law.

56. Furthermore, during the period of duration of the infringement, the complainant did not have the necessary policies in place, and this generated uncertainty in relation to the lawfulness and transparency of the controller's data protection practices and operations.

57. Accordingly, the Commissioner examined one of the key principles of processing personal data is transparency, which is intrinsically linked to the principles of lawfulness and fairness. Altogether, these principles are laid down in article 5(1)(a) of the Regulation, which provision provides that personal data shall be *"processed lawfully, fairly and in a transparent manner in relation to the data subject"*.

Article 83(2)(b) of the Regulation

58. Article 83(2)(b) of the Regulation provides that one of the general conditions is the "*intentional or negligent character of the infringement*". The Commissioner examined whether the character of the infringements committed by the controller was intentional or negligent. In its guidelines, the Article

29 Working Party[30], provides that *"[i]n general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law"*[31].

59. After identifying objective facts gathered during the investigation of the case, the Commissioner established that there is no evidence that the [redacted] had acted intentionally, although its actions indisputably demonstrate serious lack of diligence.

Article 83(2)(f) of the Regulation

60. In his assessment, the Commissioner examined the *"degree of cooperation with the supervisory authority"*, specifically article 31 of the Regulation which provides that the "*controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks*". This is also reflected in article 39(1)(d) of the Regulation, which stipulates that the data protection officer shall cooperate with the supervisory authority.

61. After considering the wording of article 83(2)(f) of the Regulation, in particular the "*degree of cooperation with the supervisory authority*", the Commissioner determined that the controller cooperated, and the requested submissions and clarifications were provided in a timely manner.

Article 83(2)(g) of the Regulation

62. In his assessment, the Commissioner noted that the controller carries out its functions and obligations in the exercise of its role of providing services and support to children, young people, and their parents[32].

63. Throughout the investigation, the Commissioner established that on the 24th May 2022, the complainant exercised the right to access personal data on behalf of her minor son with the controller. In this regard, the Commissioner noted that the affected data subject was a minor. In fact, recital 75 of the Regulation classifies children as *"vulnerable natural persons"* and recital 38 thereof provides that *"[c]hildren merit specific protection with regard to their personal data"*.

[30] Article 29 Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, (17/EN, WP 253).
[31] Ibid
[redacted]

Article 83(2)(h) of the Regulation

64. After assessing article 83(2)(h) of the Regulation, the Commissioner noted that the infringement became known to it as a result of a complaint lodged pursuant to article 77(1) of the Regulation.

The Imposition of an Administrative Fine

65. Having due regard to the factors set out above, the Commissioner concluded that the infringements which have been identified warrant the imposition of an administrative fine. In this respect, the Commissioner analysed article 21 of the Act, which states that the "*Commissioner may, after giving due regard to the circumstances of the case pursuant to Article 83(2) of the Regulation, impose an administrative fine on a public authority or body: Provided further that such a fine* ***shall not exceed fifty thousand euro (€50,000)*** *for each violation and, additionally, the Commissioner may impose a daily fine payment of fifty euro (€50) for each day during which such violation persists, which fine shall be determined and imposed by the Commissioner, in accordance with the procedure stipulated under article 26 for an infringement of Articles 83(5) or 83(6) of the Regulation"* [emphasis has been added].

On the basis of the foregoing, the Commissioner hereby establishes that the [redacted] is acting in the capacity of controller, and therefore the Commissioner decides that the controller has infringed:

a. **article 12(3) of the Regulation, for failing to provide the complainant with information on the action taken on her request to access the personal data of her minor son within one (1) month of receipt of such request;**

b. **articles 15(1) and article 15(3) of the Regulation, for failing to provide the complainant with the information concerning the processing activity and a copy of her son's personal data undergoing processing at the time of the request;**

c. **article 38(1) of the Regulation, for not properly and in a timely manner involving the DPO in the internal handling of the case;**

d. **the principle of transparency pursuant to article 5(1)(a), including article 12(1) of the Regulation, as the 'Data Protection Policy' available on the [redacted]'s website does not contain all the minimum requirements held in article 13 and article 14 of the Regulation; and**

e. **article 24(2) of the Regulation for not having in place an internal data protection notice addressed to its employees to ensure and to be able to demonstrate that the processing is performed in accordance with the provisions of the Regulation.**

In terms of article 58(2)(d) of the Regulation, the Commissioner is hereby ordering the controller:

a. **to revise the *'Data Protection Policy'* in order to ensure compliance with all the requirements set forth in article 13 and, where applicable, article 14 of the Regulation; and**

b. **to establish an internal data protection notice pursuant to article 24 of the Regulation.**

The revised *'Data Protection Policy'* shall be made available to the data subjects, and the internal data protection policy shall be made available to all the employees within sixty (60) days, from the date of receipt of this legally-binding decision, and the controller is ordered to inform the Commissioner with the action taken immediately thereafter. A read-and-sign approach is generally recommended to ensure that members of staff do indeed read the contents of the policy.

In addition, after having taken into consideration the submissions provided by the [redacted], it transpired that data protection training was not provided to all employees, and thus, the [redacted] is hereby being reminded to ensure that data protection awareness-raising and training of staff, in particular of those performing working duties involving the handling of personal data, should take place during the induction period for new employees and periodically to all the members of staff.

After assessing the criteria listed in article 83(2) of the Regulation, the Commissioner considers that an administrative fine is a necessary and adequate measure to respond to the nature and gravity of the infringement. After taking into account the second proviso to article 21 of the Act, in terms of article 58(2)(i) of the Regulation, the Commissioner hereby imposes an administrative fine of two thousand five hundred Euro (€2,500), which shall be paid within twenty (20) days from receipt of this decision.

Ian DEGUARA (Signature)
Digitally signed by Ian DEGUARA (Signature)
Date: 2023.05.04 12:42:00 +02'00'

Ian Deguara
Information and Data Protection Commissioner