idpc
INFORMATION AND DATA
PROTECTION COMMISSIONER

Our Ref: CDP/DBN/31/2020

14th January, 2022

Mr Philip Farrugia
Director
C-Planet (IT Solutions) Limited
24, Telemetry House
Conservatory Street
Floriana, FRN1520.

Subject: **PERSONAL DATA BREACH**
Hacking Attack - Unauthorised Disclosure of Personal Data

I. AWARENESS OF THE INCIDENT BY THE COMMISSIONER

1. On the 1st April 2020, the media reported an alleged personal data breach[1] (the "**breach**" or the "**incident**") suffered by C-Planet (IT Solutions) Limited[2] ("**C-Planet**"), wherein, allegedly, a database containing the personal data concerning Maltese voters had been exposed.

2. The media reported that a security vulnerability of a server (the "**compromised server**") pertaining to C-Planet had led to the exposure of over three hundred, thirty-five thousand (335,000) personal records of voters in Malta found in a database[3] (the "**compromised database**" or the "**database file**") stored on the compromised server. The same media release indicated that security researcher, [redacted], had previously detected the issue and, on the 29th February 2020, he sent an e-mail to C-Planet to inform it about the vulnerability. On the same day, he also posted on the social media platform Twitter, about the incident.

[1] Article 4(12) of the General Data Protection Regulation defines a *'personal data breach'* as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*.
[2] C-Planet (IT Solutions) Limited is a private limited company incorporated in Malta, having registered number C 41536 and its registered address at 24, Telemetry House, Conservatory Street, Floriana, FRN1520, Malta.
[3] Infra, section X.II.

3. On the 31st March 2020, the online monitoring service *'Under The Breach'* also announced the incident on its Twitter account, and it published extracts of records taken from the compromised database.

4. On the 2nd April 2020, the Daphne Caruana Galizia Foundation[4] (the **"Foundation"**) notified the Information and Data Protection Commissioner (the **"Commissioner"**) about the incident. The Foundation sustained that the database was also distributed on file hosting platforms, such as Mediafire, and provided the Commissioner with the public URL[5] on which the compromised database was made available.

II. PRELIMINARY ACTION TAKEN BY THE COMMISSIONER

5. On the 1st April 2020, C-Planet submitted a preliminary personal data breach notification pursuant to its obligation emanating from article 33 of the General Data Protection Regulation[6] (the **"Regulation"**).

6. On the same day, by virtue of article 58(2)(f) of the Regulation, the Commissioner instructed C-Planet to switch off any servers and systems affected by the incident, and to provide the Commissioner with confirmation of the action taken without undue delay. Furthermore, the Commissioner requested C-Planet to conduct an internal investigation in relation to the incident and to submit its findings in a detailed technical report. Additionally, the Commissioner requested further submissions from C-Planet, including but not limited to, system documentation and database schema.

III. APPOINTMENT OF EXTERNAL AUDITOR

7. After taking into consideration the nature of the incident, and particularly, the large number of data subjects potentially affected, the Commissioner proceeded to engage an external auditor to

[4] The Daphne Caruana Galizia Foundation is registered in Malta as a legal entity with registration number LPF-280 and as a non-profit organisation with enrolment number VO/1633.

[5] https://www.mediafire.com/file/ov5t9r4m4kfbeau/Registery.zip/file. At the time of issuing this decision, the URL shows an error.

[6] 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.

conduct a technical audit on C-Planet's IT systems. The appointed auditor was [redacted][7] (the “**auditor”**).

8. On the 8th April 2020, the Commissioner provided the auditor with a copy of all C-Planet's submissions received until that date. The auditor was assigned to carry out a fact-finding exercise, a detailed technical analysis on the evidence gathered and a thorough review of the documentation available.

9. The identified objectives of the audit were to examine and evaluate:

   a. the security measures, which C-Planet had in place, in particular, those to protect the compromised server, before it suffered the breach;

   b. the vulnerabilities in any system, server, IT and network infrastructure that led to the incident;

   c. the security measures, which were adopted following the incident, and whether these were considered to be appropriate to mitigate the risks of further security incidents;

   d. C-Planet's security policies and procedures;

   e. any interoperability between the file[8] containing the compromised database and other systems/servers, using APIs, web services, store procedures or trusting protocols, and any other similar connectivity protocols, to share information with their various clients, especially with [redacted][9] and, if in the affirmative, which data elements have been accessed, and whether the data transferred was encrypted in the communication operation; and

[7] [redacted] has its registered address at [redacted].

[8] Infra, para. 84(dd).

[9] During the investigation of the incident, C-Planet sustained that it is not the controller with respect to the processing of personal data contained in the compromised server, but rather a processor (as defined in footnote 17) acting on behalf of the controller (as defined in footnote 16), [redacted]. See infra, section VIII.

f. any form of audit trails and logging in place, including the rights and privileges associated with any data that may have been shared.

10. On the 16th April 2020, the auditor carried out an on-site inspection at C-Planet's premises. During such inspection, a meeting was held between the auditor, C-Planet's sole director and shareholder, Mr Philip Farrugia ("**Mr Farrugia**" or "**PF**"), and C-Planet's key employees. The auditor also conducted a technical analysis of C-Planet's IT systems and reviewed the documentation available, including the copy of the REXTESTDEV server[10] image saved on the 1st April 2020, which was extracted from the cloud server hosting location and stored on a PC at C-Planet's premises by a court expert[11] on the 9th April 2020.

11. On the 4th May 2020, the Commissioner received an Information Security Audit Report (the "**Audit Report**") issued by the auditor as a result of the technical audit, together with three (3) related annexes that supported the facts and findings.

12. On the 14th May 2020, during a remote meeting held between the Commissioner and the auditor, the latter presented to the Commissioner the main findings established in the Audit Report.

IV. DOCUMENTS AND SUBMISSIONS RECEIVED

IV.I Submissions provided by C-Planet

13. During the course of the investigation, Mr Farrugia acted as the contact point. Within such investigation, the Commissioner analysed the following documentation and submissions provided by C-Planet:

a. the preliminary personal data breach notification (the "**preliminary notification**") submitted by C-Planet on the 1st April 2020 at 15:13hrs, and the complete personal data breach notification (the "**complete notification**") submitted by C-Planet on the 1st April 2020 at 22:13hrs;

[10] *'REXTESTDEV'* was the C-Planet's server which was compromised during the breach. In the Audit Report, the auditor pointed out that *"[t]he server's hostname is referred to as 'REXTESDEV' in the Full Technical Report, however, according to the server logs, the actual hostname is 'REXTESTDEV'"*.

[11] Mr Farrugia filed a report with the Police on the incident. See infra, para. 17.

b. the preliminary technical report (the "**preliminary report**"), submitted by C-Planet on the 5th April 2020;

c. the full technical report (the "**full report**"), submitted by C-Planet on the 14th April 2020;

d. C-Planet's replies to the Commissioner's document *'Facts established during the IT Security Audit of C-Planet and the server REXTESTDEV'*[12]. C-Planet initially provided the Commissioner with these replies on the 29th May 2020, but then submitted a second consolidated version of the same replies on the 4th June 2020;

e. the e-mail dated the 29th May 2020 sent to the Commissioner by C-Planet's lawyer; and

f. the e-mail dated the 2nd April 2020 concerning the allegations made by C-Planet that the leaked data pertained to [redacted] [redacted][13] ("**third party company**"), a company operating in the financial sector.

IV.II Documentation provided by the auditor

a. The Information and Security Audit Report and three (3) related annexes, received by the Commissioner on the 4th May 2020;

b. The Fact Finding Report (the "**Facts Report**"), received by the Commissioner on the 19th May 2020; and

c. The auditor's responses to C-Planet's replies on the *'Facts established during the IT Security Audit of C-Planet and the server REXTESTDEV'*[14], received by the Commissioner on the 26th June 2020.

[12] This document was issued by the Commissioner on the basis of the Facts Report provided by the auditor. See infra, section XIV.I.

[13] [redacted] [redacted] [redacted] is a private limited company incorporated in Malta, having registered number [redacted] and registered address at [redacted]

[14] Infra, section XIV.III.

IV.III Submissions received from other stakeholders following a request made by the Commissioner

14. Submissions provided by the third party company in relation to C-Planet's allegation that the third party company acted as the controller in respect of the leaked data, including:

   a. the e-mail dated the 3rd April 2020 sent to the Commissioner by the third party company's lawyer;

   b. the e-mail dated the 15th April 2020 sent to the Commissioner by a representative of the third party company;

   c. the unsigned Letter of Engagement between C-Planet and the third party company dated October 2015, received by the Commissioner on the 17th April 2020;

   d. the e-mail dated the 21st April 2020 sent to the Commissioner by the third party company's lawyer; and

   e. the e-mail dated the 30th April 2020 sent to the Commissioner by the third party company's lawyer.

15. Submissions provided by the Electoral Commission, dated the 24th July 2020.

V. C-PLANET'S POSITION IN RELATION TO THE INCIDENT

16. C-Planet's principal remarks in relation to the incident are being reproduced hereunder:

   a. C-Planet stated that the company was a victim of a *"brute force entry cyber-attack"*[15] [...] *a coordinated and targeted attack of malicious origin* [...] *by a person or persons who knew exactly what they were doing* [...]". In the full report, C-Planet contended that "[...] *the only way that the person in question could find this vulnerability was if he was on a fishing expedition by scanning IPs to see if anything could be exploited. The person who carried out this targeted action on this server, did not merely identify the hole, but*

[15] All parts of this decision in italic are to be considered *ad verbatim.*

abusively copied the data from our servers before he contacted us about the 'hole' in our server. For somebody to see the data he must have accessed the hole not just identified it, download the data on his computer and run scripts to identify and read the data abusively stored";

b. with reference to the vulnerabilities identified by the auditor, both in the server REXTESTDEV and the Apache server, C-Planet argued that "[…] *we implemented these securities measures on our clients' servers. Therefore, it is important for the IDPC to note that the reason why these files were accessible was not because we do not implement the measures pointed out by* [redacted] *by default (we do) but because, through human error of a staff member* […] *the archive found its way on a server that could be accessed remotely through a direct penetration*". C-Planet further considered that "*[n]ot understanding our general security obligations and failing to implement them across the board is one thing, Human error with respect to one incident is quite another. We are not denying that this human error took place but this must be evaluated in the context of the criminal offence we suffered* […]";

c. additionally, C-Planet submitted that "[…] *the data that the media focused on (voter's details) were never even processed by us because all we did was test the potential of the customised software by having raw data at the back end. The only criteria made searchable as part of the test were non-sensitive personal data. We were always under the impression that this was simply the electoral register. The Client who provided us with the data (not* [redacted]*) never claimed that this database was created by them. We were simply instructed to 'use this file' when creating the software for them* […]. *Since the client never claimed that the file was file was proprietary in nature, and referred to it as the 'Electoral Registry' we believed it to be the same file one could obtain from the central government and this is why this was used as part of a test for another client. Otherwise, has our contact informed us that the data was proprietary, we would have left it in the* [redacted] *table. So, at the time, we genuinely believed this to be the electoral register which was freely available on CD to anyone. We stress the FACT THAT WE NEVER PUBLICED THIS DOCUMENT IN ANY WAY OR FOR or ever intended it to be made accessible remotely* […]".

17. Throughout the investigation, Mr Farrugia repeatedly sustained that C-Planet was the victim of a cyberattack, which constitutes a criminal offence. During the night between the 31st March 2020 and the 1st April 2020, C-Planet lodged a report with the Malta Police Force (the "**Police**") in relation to the incident. Mr Farrugia also personally contacted the Police Cyber Crime Unit to explain the actions taken thereupon, such as switching off all C-Planet's servers including those used for its clients.

VI. INCIDENT TIMELINE

18. In the full report, C-Planet confirmed, that *"[t]he above-described vulnerability was detected on the 29th of February 2020 by an individual* [...] *who contacted* ***us by email at 17:18 on 29th February 2020*** *stating that we had a hole in our server and that we should fix it and attached two screenshots"* [emphasis has been added].

19. C-Planet declared that it *"took this information to heart and investigated the issue on the server whilst taking all precautions to avoid giving this 'good Samaritan' any data he may have been fishing for. The directory was locked by a username and password* [...]. *The username and password were in place by the 5th of March* [...]*"*.

20. C-Planet remarked that, as shown in those screenshots, "[...] ***this individual downloaded the file on his local machine*** [...]*"* [emphasis has been added]. According to C-Planet's Director, *"[t]he full extent of what was being done by the hacker who seemingly was pretending to act in good faith (as a 'white hat hacker') was not revealed to me until I received a message from one of my clients telling me to have a look at the tweet dated 31st of March 2020"*.

VII. LIFTING OF THE PROCESSING BAN ON C-PLANET'S SERVERS

21. On the 9th April 2020, the Commissioner temporarily lifted the processing ban on C-Planet's compromised server to allow the Police to gather the necessary evidence for the purpose of its investigation, and instructed C-Planet to switch off the servers once again, immediately following the conclusion of the Police's activity.

22. On the same day, the Commissioner lifted the ban on C-Planet's servers which were not compromised by the breach.

VIII. THE POSITIONS OF C-PLANET AND THE THIRD PARTY COMPANY IN RELATION TO THE PROCESSING OF PERSONAL DATA CONTAINED IN THE COMPROMISED SERVER

23. On the 2nd April 2020, C-Planet sent an e-mail to the Commissioner claiming that it was not the controller[16] with respect to the processing of personal data contained in the compromised server, but rather a processor[17] acting on behalf of another controller.

24. C-Planet reiterated the same argument during the audit, whereby it submitted that "[...] *the electoral register data that was quoted in the press articles was provided to C-Planet by a client* [redacted]*) for use in the software that C-Planet was developing. PF also stated that his impression of this database was that it is the same dataset that could be acquired from the Electoral Commission. When asked why it was found in several projects on the development server*[18]*, PF stated that it was used in the past as a "template" for various software projects to different clients"*.

25. In addition, in both the preliminary and complete notifications, C-Planet sustained that *"[t]he file databasebkp.sql was a file supplied by one of our customers in order to harmonize his data when we were given the task of creating new software for his company* [...]*"*. Later on, when rebutting the auditor's findings[19], C-Planet also stated that *"the file in question was given to me by a specific individual who no longer works at* [redacted]". On the 2nd April 2020, C-Planet clarified that they were actually the processor and not the controller in respect of the incident in question.

26. The Commissioner specifically requested the auditor to examine whether there was any evidence within C-Planet's IT systems to demonstrate that the file *'databasebkp.sql'* was supplied to C-Planet by the third party company. In this regard, the auditor also analysed all databases for any interoperability or association to the electoral register dataset and concluded that "[...] [redacted] *databases* ***do not contain any specific stored procedure with references to the 'Elec_Registery' database or any data set stored within the latter*** [...]" [emphasis has been added].

[16] Infra, para. 90.
[17] Infra, para. 97.
[18] The server REXTESTDEV.
[19] Infra, section XIV.II.

27. On the 3rd April 2020, the third party company, through its lawyer, submitted to the Commissioner that C-Planet indeed provided it with IT services, but that it had "*no association with the 335,000 records of personal data allegedly exposed by C-Planet*".

28. On the 6th April 2020, the Commissioner requested the third party company to submit a copy of the agreement concluded pursuant to article 28(3) of the Regulation between both parties governing the data processing activities connected to the provision of IT services. The Commissioner indicated that, in the event that such agreement was not available, a copy of any other agreement or contract which was available and governed the services rendered, should be provided.

29. On the 15th April 2020, the third party company informed the Commissioner that the only document that could be traced was an unsigned contract dated 2015. A copy of this contract was requested by the Commissioner and provided on the 16th April 2020.

30. On the 20th April 2020, upon reviewing the unsigned contract, the Commissioner requested the third party company to provide further information and clarifications, *inter alia*: (a) information about the migration of data from the company's ICT systems to [redacted] ICT system; (b) to confirm whether the contract was still in force; and (c) to specify whether C-Planet was providing additional services involving any processing of personal data.

31. By means of an e-mail dated the 21st April 2020, the third party company provided the following responses:

    a. that "*[t]he company's management has no direct personal knowledge as to its circumstances, other than to state that it was forwarded to the Company by Philip Farrugia of C-Planet when my clients enquired as to the existence of any written agreement between the parties. Since they have not managed to trace a signed copy, they can only assume that it was never endorsed. Management cannot confirm whether it was the intention of the company at any time to accept the conditions proposed in the agreement text recently received. It is safe to state, in any case, that the text did not originate at* [redacted] *end* [...]";

b. that *"[m]y clients confirm, however, that C-Planet did implement the migration of data to* [redacted]*'s ICT system. This took place when, in 2016,* [redacted] *replaced its principal* [redacted] *with* [redacted]*.* [redacted] *were using an IT system custom-developed by C-Planet* [redacted]*, who also supported it. The migration took circa four months* [...]";

c. that *"[s]ince then, C-Planet have continued providing support of the bespoke* [redacted] *system developed by them, and general office IT operations including email support, configurations, cloud storage and user management* [...] ";

d. that *"[i]n the light of recent developments, however,* [redacted] *stopped requesting C-Planet's services. "*; and

e. that *"[m]y clients make specific reference to your question regarding data on "about 328,644 voters, including their voting leaning". They have no knowledge of such data, and never had any reason to hold, use, or ask anyone to process said data".*

32. On the 25th April 2020, the Commissioner sought further clarifications from the third party company to define: (a) the business relationship between them and C-Planet; (b) the types of personal data which were migrated to [redacted] ICT System; (c) the purposes and categories of personal data processed within the system [redacted]; and (d) what other support services were provided by C-Planet to the third party company.

33. On the 30th April 2020, the third party company responded to the Commissioner's request by providing an invoice dated the 9th October 2014 (no. [redacted]) and other job sheets related to the provision of IT support services by C-Planet. It further held that:

a. the invoice appeared to be the earliest document held in their records, even though C-Planet had developed software prior to the date of such invoice;

b. C-Planet provided ongoing technical support, however there was no signed agreement which could be traced in relation to the migration to [redacted] ICT system;

c. the data object of the migration related specifically to the business of [redacted] in the context of the transition to [redacted]'s system from [redacted];

d. [redacted] was a[redacted] business software system developed by C-Planet for the third party company, for which, there was no specific documentation. Training on the system was, at the time, provided by the developer;

e. [redacted]; and

f. IT support was provided on an ongoing basis, without a specific written undertaking.

34. On the 21st May 2020, the Commissioner requested C-Planet to provide substantial evidence to support and corroborate the claim that C-Planet was a processor acting on behalf of the third party company, in respect of the processing operation affected by the incident. C-Planet failed to provide concrete evidence to effectively demonstrate that it was acting in the role of a processor for and on behalf of the third party company, in relation to the compromised database.

IX. CONSULTATION WITH THE ELECTORAL COMMISSION

35. On the 21st July 2020, as part of the investigation of the incident, the Commissioner held a consultation meeting with the Electoral Commission.

36. Following such meeting, by means of a communication dated the 24th July 2020, the Electoral Commission submitted the following written considerations:

"[t]he scope of the meeting was to:

- *Check and verify data extracted from a data file elevated by the IDPC (hereinafter referred to as "IDPC data") during the investigation of the data breach believed to include electoral data pertaining to general and local councils' elections held in March 2013, and compare it with data stored in the computer system of the Commission (herein after referred to as "source data");*

- *Determine and conclude whether the IDPC data is identical to the source data;*

- *Confirm with the CEC* [Chief Electoral Commissioner] *whether the source data contain other data elements such as telephone numbers and other values; and*

- *Confirm the third parties to whom the source data was provided.*

[...]

Both files (IDPC data and source data) used for comparison purposes were in Excel format and therefore Excel comparison functions and tools were used to ascertain whether the data in question are identical. The file provided by the IDPC to the Commission contained ***337,384*** **[three hundred thirty-seven thousand three hundred eighty-four]** ***records*** *including ID Card numbers pertaining to non-Maltese citizens ('A' ID Card numbers) and a number of null records which were eventually deleted in the matching process.*

In view that IDPC data included ID Card numbers ending with an 'A', it was concluded that the data pertained to both 2013 Local Councils' elections and 2013 General Elections held on the same day: 9th March 2013.

The data was compared as shown in the attached sample screenshots, data matched perfectly with the data extracted from the Electoral Commission's computer system.

It should however be noted that the data elevated by yourselves is incomplete and does not reflect in its entirety the electoral data extracted for the 2013 elections.

This same data was forwarded to the Political Party Delegates prior to the said elections as permitted in Article 10(5) of Chapter 354 (General Elections Act) of the Laws of Malta";

I also confirm that ***the computer system does not hold other data such as telephone numbers of voters and therefore no such data was provided by the Commission to the party delegates mentioned above*** " [emphasis has been added].

37. At the end of the data matching exercise, in order to preserve the integrity of the data, the Commissioner and the Electoral Commission agreed to keep a copy of both files used, which

were saved on a USB drive, sealed in an envelope duly signed by both representatives and kept in a secure place to be opened only if required in any eventual legal proceedings.

X. CIRCUMSTANCES OF THE INCIDENT

X.I. Systems affected by the incident

38. Following the thorough audit conducted by the auditor, which included an on-site inspection, it was ascertained that C-Planet's IT infrastructure consisted of employees' workstations connected to a local network. The auditor reported that the server infrastructure was located on a cloud hosting platform provided by [redacted] [redacted][20] ("[redacted]"), where the compromised server, named *'REXTESDEV'*, was hosted.

39. Whilst the auditor sustained that the compromised server appeared to be **both a test and development server**, on the contrary, in its submissions, C-Planet maintained that *"[t]he server REXTESDEV was set up to be a repository of php files which are the source code of programs that are in development for our clients* [...]*"*. C-Planet also held that *"[t]he server REXTESDEV was first set up about 8 years ago on a local virtual hosting environment* [...] *which was deployed on a* [...] *server that was installed in the rack of the office server room. The server was only accessible by pcs on the local network. The local network was secured using a* [...] *firewall and network was given to the device through an HP switch. About 2 years ago the server's raid controller*[21] *developed a fault and as the RAID controller stopped functioning, it was decided that all the virtual servers hosted on the* [local] *hosting environment were to be transferred to the cloud servers that we are still using to this day* [...]*"*. C-Planet also maintained "[...] *that following the fault, an exercise using a live instance of 'ubuntu server' was used in order to recover the lost data from the physical server. We managed to recover the database from the MDF file and generated a dump file so that it could be imported onto the cloud server. Although the dump file was not entirely complete, we could still recover the majority of the database and*

[20] [redacted].

[21] A disk array controller is a device that manages the physical disk drives and presents them to the computer as logical units. It almost always implements hardware RAID, thus it is sometimes referred to as RAID controller. It also often provides additional disk cache.

clients' files were secured with no issues. ***However, this dump file remained unintentionally in the system***[22] " [emphasis has been added].

40. In addition to the above, C-Planet stated that *"[t]he server REXTESDEV was deployed with all the configuration and data (as is). The security that was set up on the new cloud deployment was a point-to-point locking that allows only connections that originate from one of the office static IPs. The service for the internet connection was and is still provided by* [redacted]. ***In November 2019 we decided to change the type of service from a*** [...] ***static ip to a*** [...] ***single dynamic ip.*** *This decision was taken due to the fact that we did not have any local servers that were hosted on our local network anymore. The server REXTESDEV* ***was set to be hardened and secured before the point-to-point security was removed. The hardening on the server was completed and the point-to-point security was removed and the fixed IPs of the office were removed*** [...] " [emphasis has been added].

X.II. Object of the incident

41. The object of the incident was an SQL script file named ***'databasebkp.sql'***, which the auditor found in the directory ***'/var/www/html/_ARCHIVE'*** of the REXTESTDEV server. The database file contained certain categories of personal data pertaining to three-hundred thirty-seven thousand, three hundred eighty-four (337,384)[23] data subjects, as further elaborated below[24].

X.II.I. The position of C-Planet in relation to the database file

42. In relation to the database file, C-Planet submitted *inter alia*:

    a. that *"[t]he file databasebkp.sql was found on the test server REXTESDEV with ip* [redacted] *under /var/www/html/_ARCHIVE folder* [...] ";

[22] Infra, para. 42(c).

[23] The Commissioner found a discrepancy between the number of affected data subjects indicated by C-Planet and the information gathered by the Commissioner during the course of the investigation. The Commissioner established the figure 337,384 according to the findings established by the auditor, which figure was also confirmed by the Electoral Commission.

[24] Infra, section XV.II.

b. that "*[t]he file databasebkp.sql was a file supplied by one of our customers in order to harmonize his data when we were given the task of creating new software for his company. The Source code and SQL file were archived back in 2013. Databasebkp.sql is not voter data, it something not related to voters data*";

c. that the database file was "*a three-years old, "forgotten" backup SQL file*", defined as "*a sql dump file*". C-Planet held that "*[t]he sql file was created in 2018 after the local database server installed on our local network, generated a fatal error due to a faulty raid controller* [...]". Additionally, C-Planet claimed that it was able to retrieve a disc image of the original database and to convert such image disc into the database file in question. In its full report, C-Planet declared that the file was a "*temporary file created on the server and is not a true backup of the database even thou the name would suggest otherwise* [...]". In this regard, C-Planet confirmed that "*[t]he file contained the data that was then published on news portals* [...]";

d. that in the folder '*votingDocumentSystem*' mentioned by the media, found in the '*/var/www/html/_ARCHIVE*' directory, "*there is no personal data stored it only holds source code which is proprietary to our company and we keep the right to keep a copy of the source code. There is no SQL dataset related to the voters' data* [...]. *This code was used for a client* [[redacted]], *that requested* [redacted] *for a* [redacted] *and was used between the* [redacted] [redacted] *till the exercise was over. This dataset was only accessible by us. Once the* [redacted] *was carried out on the* [redacted], *we used the data to generate a report for the client* [...]. *For the said project we only had access to* [redacted] *data and this dataset was not within our local area network but on the cloud. We never had any voters database external to* [redacted] *stored on our local servers* [...]"; and

e. that additionally, C-Planet only had access to the [redacted] [redacted] data in real time, and that the data was returned to the [redacted] once the task was finalised. C-Planet further stated that the data was kept in a virtual cloud server provided by [redacted], and that the same data was eventually destroyed.

X.II.II. The sets of electronic data examined by the auditor

43. The auditor identified, following an analysis of the REXTESDEV server image, the following main sets of electronic data, which it subsequently examined:

a. *"[t]he directory /var/www/html containing files that were served by the web server to the Internet. This directory contains further subdirectories relating to projects that C-Planet worked on including files that were created or amended during 2020";*

b. *"[t]he subdirectory /var/www/html/_ARCHIVE containing a set of directories and files that C-Planet indicated were related to projects that were no longer active. In these sub-directories, database script files (.sql) were found containing database tables and data of projects at different points in time";* and

c. *"[t]he SQL script file 'databasebkp.sql' found within the /var/www/html/_ARCHIVE directory, containing database tables and data that were extracted from a faulty server in 2017*[25]*. The latter was replaced by the REXTESDEV server set up on a cloud hosted environment* [redacted] *by C-Planet* [...]*".*

X.II.III. The auditor's findings in relation to the database file

44. In the Audit Report, the auditor made *inter alia*, the following observations:

a. during the analysis of the data in the server REXTESDEV, *"several instances of the electoral register dataset and its related uses were found. Two databases on the live MySQL server, 'Elec_Registery' and* [redacted] *contained the identical 330k records that existed on 'databasebkp.sql', while a subset of 29k records was found in another database 'Elec_Register*[redacted]*'* [...]". The auditor remarked that *"[f]urthermore, REXTESDEV was found to contain confidential and real personal data in various locations and databases* [...]*";* and

[25] According to C-Planet, the database file was created in 2018.

b. at the time of obtaining a copy of the server image, the MySQL database service installed on REXTESDEV server contained databases that were *'live'* (stored within *'/var/lib/mysql'*).

XI. TECHNICAL AND ORGANISATIONAL MEASURES IN PLACE BEFORE THE INCIDENT

XI.I. Security measures in place on the compromised server

45. The first objective of the audit was to establish *"[w]hat security measures the Company had in place, in particular, those to protect the compromised server, before it suffered the breach*". In essence, the auditor conducted an analysis to establish whether the technical and organisational measures adopted by C-Planet at the time of the incident were in compliance with information security industry's best practices and whether such measures were appropriate to protect the integrity and confidentiality of the personal data contained in the compromised server, considering the risk posed by the processing. The methodology used by the auditor was to enumerate the root directory and its respective subdirectories within the server image of REXTESDEV to analyse the system, the applications and the configuration files. As a result of such analysis, the auditor reported that at the time of the incident, C-Planet had the following security measures in place:

XI.I.I. Strong root password

46. In relation to C-Planet's statement that *"a **16-character complex password** generated from* [redacted] *was in use for the 'root' account"*, the auditor held that it could not verify such statement, because the obtained copy of the server image was secured by a different password configured by the court expert.

XI.I.II. LAMP stack

47. The auditor found that at the time of the audit, the web server stack comprised of Linux, Apache, MySQL, and a PHP engine, abbreviated as LAMP, which was relatively up-to-date, with the exception of the PHP engine.

XI.I.III. Services running with low privileges

48. The auditor found that *"[s]ervice daemons running on the compromised server were identified to be running with low privileges, minimising the risk of a quick system escalation of privileges in the event of service compromise"*.

XI.I.IV. No custom SUID/SGID programs

49. The auditor established that the compromised server did not contain any non-system programs with SUID/SGID permissions[26] that were worth analysing for any possible vulnerabilities.

XI.I.V. Logging facility

50. The auditor found that *"logging was enabled on the REXTESTDEV for the Linux system as well as important services such as SSH authentication, Apache and MySQL* [...] *"*, and acknowledged the statement of C-Planet that the log retention policy was set to thirty (30) days by the cloud hosting platform provider, which according to the auditor *"hindered the ability to investigate logged activities during the period when the incident took place as it happened more than 30 days prior to 1 April 2020"*.

XI.I.VI. AppArmor

51. The auditor found that AppArmor[27] was installed and running on the compromised server.

XI.I.VII. Network security

52. The auditor found that *"[n]o network security measures were found to be present to filter and protect the server machine from unwanted network traffic. Host-based network security measures only included a* ***default configuration of 'iptables'****"* [emphasis has been added].

[26] SUID/SGID permissions allow users to temporarily run other programs with another user's privileges, normally that of the root account. If configured incorrectly, the SUID/SGID permissions may open a system to privilege escalation vulnerabilities.

[27] AppArmor is a Linux kernel security module that restricts program's capabilities through app-specific profiles and enforced via Mandatory Access Control (MAC).

A

XI.II. Vulnerabilities that led to the incident

53. As a second objective of the audit, the auditor was instructed to designate *"[t]he vulnerabilities on any system, server, IT and network infrastructure that led to this incident*". As a result of that exercise, the auditor found *inter alia* that "***no network security measures were in place to protect the REXTESDEV server from a direct intrusion attempt***", and it further identified "*specific security misconfigurations on the server that are contributing vulnerabilities that* ***allowed for this incident to materialise***" [emphasis has been added]. The auditor concluded that "***the evidence indicates that the data breach was a result of a lack of security on the contents of the Apache server directory that left an open door for intruders to download any data it contained***" [emphasis has been added]. An overview of the vulnerabilities identified by the auditor are being reproduced in the following sections.

XI.II.I. Indexable website

54. Taking into account that *"[s]earch engines use web crawlers to identify publicly accessible websites and web resources and index them accordingly*", the auditor noted that the compromised server was not resolvable by a domain name, but still remained indexable by search engines that index websites through an IP address only. In this regard, the auditor added that *"[t]he compromised server did not appear to have the robots.txt file*[28] *set*" or "*alternatively the 'noindex' directive*[29] *(configured in the Apache web server)"*, and concluded that *"since the IP address of the server was not linked to a domain name, the intruder had to knowingly access the web server through the knowledge of the server's public IP address. It is possible that automated web-crawling software could have detected "interesting" data files such as ".sql" files and flagged them for further (human) examination* [...]*"*.

XI.II.II. Missing default index file

55. Giving due regard to the fact that *"[b]y default, web servers are configured to prevent directory listing by showing the default index web page, e.g. 'index.html', when no specific resource in a*

[28] Robots.txt files contain instructions for search engine crawlers about which pages should or should not be indexed.

[29] *'noindex'* is a configuration that completely blocks search engines from indexing the websites on the server.

directory is requested by the end user/browser", the auditor found that "*[t]he default index file*[30] *on the Apache server document root was not present (/var/www/html) and other directories, thus allowing any unauthenticated users to access directory contents on the web server simply through the knowledge of the IP address* [...]".

XI.II.III. Directory listing not disabled

56. In conjunction with the missing default index file, the auditor found that "*the directory listing feature on the Apache web server was enabled in the configuration file and, thus, a listing of the directories contained within the document root is automatically shown to the end user due to the missing index file*". The auditor observed that "*[t]herefore, "the /var/www/html/_ARCHIVE/ directory within the compromised server was made easily accessible, allowing the intruder to download files stored inside the web server directory structure, including the 'databasebkp.sql' file*".

XI.II.IV. Lack of authentication mechanism

57. The auditor found that "*[f]urther to the accessibility of the directory listing, no form of authentication was configured to protect the unauthorised disclosure and eventual misuse of resources stored within the web server directory structure. This can be achieved by configuring Basic Authentication on the Apache web server, which would also have prevented the website from being indexable by search engines*".

XI.II.V. Network security

58. The auditor established that "*[t]he REXTESDEV server was configured to expose all required services directly to a public IP address, as identified within various configuration files. This implies that the server had no network security infrastructure protecting it from a direct attack, such as by using a firewall, an intrusion detection system, VPN gateway, or some other form of a bastion host* [...]".

[30] By default, web servers are configured to prevent directory listing by showing the default index web page, e.g. '*index.html*', when no specific resource in a directory is requested by the end user/browser.

4

XI.II.VI. Personal data within C-Planet's databases

59. The auditor observed that *"[p]ersonal data is still active within the live MySQL test database. Besides the databases mentioned in Section 4.5, the majority of the other databases were also found to contain sets of seemingly real personal data, such as "voters' data" within the 'votingSystem' and 'Elec_Registery_*[redacted]*" databases,* [redacted]*. **This contradicts with statements made by PF where it was claimed that only dummy data is used for development and test purposes, as well as that personal data for certain clients was destroyed once the project works were finalised*** [...]". Subsequently in the Audit Report, the auditor declared that *"[t]he 'elec_registery' also contained an empty table called 'full_details' with the same fields, but with the addition of a field 'age' that is auto calculated via the 'DoB' field. The* [redacted] *database contained a stored procedure 'Get_By_IDCard'* [...] *which performs a simple lookup by searching through the 'registery' table (within the respective database from where it is called) and retrieves a row of data that matches the given 'ID Card' (number) value. The 'elec_registery' database also contained the same stored procedure, 'Get_By_IDCard', but an error stating it is empty is prompted on the screen when accessed"* [emphasis has been added].

XI.III. Other vulnerabilities

60. In addition to the above, the auditor identified other security weaknesses on the compromised server consisting in misconfigurations, poor security practices and proper administrative oversight which, in its view, made the same compromised server susceptible to various attack vectors. The auditor clarified that, whereas such weaknesses ran contrary to industry standard server hardening security practices, they did not necessarily contribute to the security incident in question. An overview of these additional vulnerabilities is outlined below.

XI.III.I. Outdated Linux kernel

61. The auditor established that the Linux kernel version running at the time of the incident was relatively old[31].

[31] Version 4.4.0-127-generic, released on the 19th May 2018. The auditor observed that the most recent version at the time of the report was 4.4.0-177, released on the 15th March 2020.

XI.III.II. Apache service weaknesses

62. The auditor found that *"[t]he Apache web service was found to contain various following security misconfigurations which increase the attack surface against the server:*

a. *Version banner was returned to connecting user, exposing service name and version to the public Internet;*

b. *Service allowed to run over HTTP on* [redacted] *(common for general public use but not necessary for development/testing environment);*

c. *The insecure protocols TLSv1.0 and TLSv1.1 are supported;*

d. *HTTP method 'OPTIONS' allowed (this should only be enabled for debugging purposes)".*

XI.III.III. MySQL service weaknesses

63. According to the auditor, *"[t]he MySQL database service was found to contain various security misconfigurations or other misconfigurations that compromise the security of the database service itself:*

a. *Service configuration shows that the service was bound to the server's public IP address, i.e. exposed on the public Internet, without any compensating controls such as the configuration of TLS or the use of a virtual private network (VPN) tunnel to encrypt (personal) data in transit.*

b. *Database engine 'root' account (this is different from the system's root account) was configured with a weak password.*

c. *The all-powerful 'root' password can be leaked from a compromise of the web server as it is hardcoded in database connection strings inside PHP files pertaining to the clients' test software located within the web server document root.*

d. *No low-privileged database accounts were configured for database access to partition the numerous clients' test databases found on the database server. A compromise of one web application means that an intruder can potentially access all other clients' databases saved on that server, unrestricted.*

e. *No 'general query logging' enabled to maintain an audit trail of access and/or changes to data*".

XI.III.IV. <u>SSH service weaknesses</u>

64. In the auditor's views, *"[t]he SSH remote access service was also found to be configured with poor security practices:*

a. *Service is exposed publicly without any compensating controls to minimise the attack surface such as rate limiting authentication requests, or otherwise exposed locally and accessed via VPN only.*

b. *Service allows direct 'root' logon with password only (a weak form of authentication for the all-powerful considering it may be accessed over the Internet)"*.

XI.IV. Auditor's conclusions in relation to the reported vulnerabilities

65. The auditor concluded that *"**the lack of security hardening on the Apache web server made it easy for the perpetrator to access the server, as well as to download any data present in the system at the time, including data pertaining to C-Planet's clients**. The consequence of the exposed system was exacerbated because real data was used within the test server, and without any privacy enhancing technologies such as encryption and anonymisation. In addition, poor secure software development practices allowed the perpetrators to lift cleartext passwords still active since 2017, the latter being evidence of lack of password policy enforcement, and subsequently use them to successfully log onto client systems hosted elsewhere"* [emphasis has been added].

XI.V. C-Planet's security policies and procedures

66. As part of the audit, the auditor was also tasked by the Commissioner to examine and evaluate the security policies and procedures implemented by C-Planet at the time of the incident. The findings of the auditor in that respect are reported hereunder.

XI.V.I. Policies, procedures and practices

67. The auditor observed that C-Planet did not have *"any documented security and privacy policies or formal procedures. Evidence of security and privacy practices were also found to be lacking, such as conducting some form of* ***risk assessments and regular security testing and assessments****"* [emphasis has been added]. Due to the fact that the organisational structure of C-Planet consisted of "*PF as the owner and Managing Director, and three other employees each covering a specific activity within the company's operations: (i) software development; (ii) network and infrastructure; (iii) IT support*", the auditor concluded that *"[s]uch a small team working in one room allows for frequent communication and consultation, albeit informal and undocumented"*.

XI.V.II. Identity and access management

68. The auditor found that *"C-Planet adopts an informal approach to identity and access management due to the size of the organisation"* and that *"no technical enforcement through some form of corporate directory service was observed"*. Additionally, the auditor found no evidence to demonstrate that granted access rights were periodically reviewed. As part of the analysis, the auditor detected certain highly privileged super-user accounts. As of physical access to C-Planet's premises, the auditor acknowledged C-Planet's statement that authorisation was required for staff to visit the premises outside office hours and for work laptops to be used by staff for the purpose of remote working and that physical access was controlled by means of [redacted] which were out-of-order at the time of the audit.

XI.V.III. Asset management

69. Insofar as asset management is concerned, the auditor found that "*C-Planet does not have an official list of their servers, workstations, allowed tools for development and other components*

which are critical for their business operations" and that *"[f]or cloud-based assets hosting the internal development environment, C-Planet relies on the asset list within cloud service provider portal. User equipment in limited to individual staff PCs";*

XI.V.IV. Secure software development and changes

70. In relation to secure software development and changes, the auditor confirmed that *"C-Planet does not follow established secure coding standards to develop and maintain their clients' software and business applications* [...]*"* and that, consequently, " [...] *the test environment was found to be publicly accessible, contains resources and files from various clients without proper segregation at system and database level, and database security is low, for example, various passwords stored as cleartext"*. In addition, the auditor stated that "[...] *the server REXTESDEV was found to contain live data including several sets of personal data"* which were not protected by "*privacy enhancing technologies, such as encryption, obfuscation, pseudonymisation and, or data minimisation to limit the impact of privacy breach*". On the other hand, the auditor acknowledged that, at the time of the audit, C-Planet was making use of a software development tracking tool named [redacted] "*which can track all software development changes, manage source code version control, version rollbacks, integration with public APIs, as well as a variety of security modules such as Active Directory integration and password hashing*". The auditor also found that "*good IT practices are followed when infrastructure changes are implemented such as off-peak scheduling and rollback plans. Documentation of the latter is not formally maintained, although a job sheet is used in the case of client servicing*".

XI.V.V. Business continuity management

71. The auditor found that *"C-Planet does not have policies, standards, high-level workflows or checklists related to business continuity management such as for incident response and disaster recovery"* and acknowledged C-Planet's statement that full server back-ups were taken to a cloud-based backup service on a daily basis. The auditor *"observed practices in terms of providing level 1 and level 2 support for troubleshooting related to their IT services offered to clients"* and found that *"[s]uch practices were found to have no relevance to privacy and security incident handling and response"*.

XI.V.VI. IT Security Operations

72. The auditor found that there were *"no documented IT security operations and working practices, nor any checklists to guide C-Planet in delivering services in a consistent and a secure fashion. In addition, the test server, which was the subject of the breach, was found to have several security issues that could expose the server to various threats* […]. *Procedures related to maintenance and monitoring of logs were also found to be inadequate or lacking, thus, hindering C-Planet's ability to detect a data breach"*. Nonetheless, on a positive note, the auditor noted that *"C-Planet has invested in tools for software development, hosting and backup of client data, although it is questionable whether such procedures are streamlined across all clients"* and that *"C-Planet have also transferred most of the inherent risks to physical security by outsourcing services to the cloud, and the bare minimum infrastructure is used on-premises"*.

XI.V.VII. Endpoint Security

73. The auditor observed that *"C-Planet has minimal security controls on its workstations, which are a mix of Linux and Windows systems. Technical security policies are, therefore, decentralised and at each system's user discretion. Standard anti-malware solutions are used without any centralised management to ensure timely signature updates or monitoring. In addition, no technologies to centralise patch management is used for servers and workstations"*.

XII. TECHNICAL AND ORGANISATIONAL MEASURES IMPLEMENTED TO ADDRESS THE INCIDENT

74. In its full report, C-Planet declared that, on the 29th February 2020, which is the time when C-Planet was first made aware of the vulnerability which led to the incident, had taken the following action: *"[t]he directory listing was locked by a username and password, and a plan was set in motion to lock the server even more. The username and password were in place by the 5th of March 2020, not as indicated in the media, and a plan was also initialized to increase the security on the connections to the server and to remove the _ARCHIVE folder from the server* […]*"*.

75. The assessment of the security measures adopted by C-Planet to address the incident and the determination of whether these measures were indeed considered appropriate to mitigate the risks

and prevent similar incidents from occurring, was another objective which the auditor was tasked to carry out. In the Audit Report, the auditor acknowledged that *"[f]ollowing the security breach, C-Planet implemented several changes to the IT environment security posture, including* [redacted] [...]". For the purpose of that analysis, the auditor distinguished between the security measures which were implemented by C-Planet following the incident and the measures which were still work-in-progress at the time of the Audit Report.

XII.I. Implemented security measures

76. The auditor acknowledged that *"security policies have been written, following the incident*" and it "*examined an electronic copy of the policy documentation titled "Policies version 1.0" dated 21 April 2020, which were found to cover a large spectrum of security domains such as network security, internet and email usage, and remote access to name a few"*. The outcome of such analysis was that [redacted] [...]".

77. Furthermore, C-Planet shared with the auditor another document titled *'Network Changes Report version 1.0'* dated the 25th April 2020. According to the auditor, such document *"describes the network-related changes and applied security measures, as explained by PF. The document details how C-Planet transitioned from* [redacted] *to a relatively* [redacted] *with various security enhancements* [...]". Together with that document, C-Planet provided the auditor with information about additional security measures implemented on different servers.

78. After having examined the documents and the information provided by C-Planet in relation to other security measures which were implemented, the auditor pointed out that *"C-Planet is on*

[redacted]".

79. On a concluding note, the auditor remarked that "[redacted]" [emphasis has been added].

XII.II. Security measures in progress

80. During the audit, C-Planet mentioned that certain measures intended to improve the security posture of the organisation were in progress. Hence, those could not be verified by the auditor during the audit. With specific reference to the [redacted], the auditor pointed out that "[…][redacted] […]". The auditor concluded its assessment by listing down certain non-exhaustive high-level recommendations, to be adopted by C-Planet prior to switching on again the compromised server.

XIII. C-PLANET'S STATEMENTS MADE DURING THE AUDIT

81. During the course of the audit, C-Planet made the following principal statements:

a. that "[…] *all employees had enrolled in GDPR-related online training in the past, a clear-desk policy is adopted within the office space, and that physical documents are securely disposed of. Confidentiality clauses were also observed within the employment contract addressing security concerns such as the unauthorised copying of data outside of company premises and handling of information assets upon termination, among others";*

b. that the "[…] *access is based on individual trust within the organisation";*

c. that the "[…] *authorisation is required for personnel to visit the premises outside office hours, while work laptops are issued for remote working. Furthermore, physical access control is used* [redacted]*, however, PF stated that the access control system was out of order at the time of the audit";*

d. that the "[...] [redacted]*, C-Planet relies on the asset list within cloud service provider portal. User equipment in limited to individual staff PCs";*

e. that the "[…] *dummy data or altered data is used during development and testing to remove confidentiality risks*"[32]*;*

f. that "[…] *each member of the team is responsible for a specific role as per their employment contract and access is granted on a need-to-know basis* […]"*;*

g. that the "[…] *daily full server backups are taken* [redacted] […]"*;*

h. that the "[…] *practices improved over the years as lessons were learnt, such that newer solutions had better security functions that older ones.* [redacted] […]"*;*

[32] On the contrary, the auditor found that real personal data was used. See supra, para. 44(a), 59 and 84(bb).

i. that "[redacted]. *PF stated that security measures are enforced through the* [redacted]*, such as requiring a* [redacted]*"*;

j. that the database within the live MySQL *"was used in the past as a "template" for various software projects to different clients, and that his impression of this database was that it is the same dataset that could be acquired from the Electoral Commission* [...]*"*;

k. that "[...] *the 'votingSystem' database for the 'votingDocumentSystem' software was specifically developed for the* [redacted] [...]*"*;

l. that "[...] *unfortunately, the log retention policy was set to 30 days automatically by the cloud hosting platform provider and this hindered the ability to investigate logged activities during the period when the security incident took place as it happened more than 30 days prior to 1 April 2020"*;

m. that *"[a]ll software we develop have* [redacted]*"*;

n. that the "[...] *security policies have been written, following the incident* [...]*"*;

o. that "[...] *the electoral register data that was quoted in the press articles was provided to C-Planet by a client* [redacted] *for use in the software that C-Planet was developing*";

p. that "[...] *a 16-character complex password generated from* [redacted] *was in use for the 'root' account* [...]*"*; and

q. that *"[t]he REXTESDEV was used as a test server for showcasing software projects to C-Planet clients"*.

XIV. THE AUDITOR'S FACTS REPORT AND C-PLANET'S REBUTTAL

XIV.I. The Auditor's Facts Report

82. On the 16th May 2020, the Commissioner requested the auditor to prepare a summary of the main findings established during the audit. The auditor therefore produced a *'Facts Report'*[33], on the basis of which the Commissioner created a document titled *'Facts established during the IT Security Audit of C-Planet and the server REXTESTDEV'*.

83. On the 21st May 2020, the Commissioner shared a copy of the aforesaid document with C-Planet to provide it with the opportunity to comment thereupon. The Commissioner clarified that, where C-Planet had reasons to disagree, it should have provided clear explanations on the reasons for the disagreement, supported by valid and concrete evidence. The Commissioner instructed C-Planet to submit its observations by the 29th May 2020.

XIV.II. C-Planet's rebuttal to the auditor's Facts Report

84. On the 4th June 2020, C-Planet submitted their counter arguments to the *'Facts Report'*. These have been reproduced hereunder, except for certain arguments put forward by C-Planet which overlapped with some of the statements previously made by C-Planet during the audit.

   a. C-Planet confirmed the composition of the employees' team;

   b. in relation to GDPR training, C-Planet attached an invoice issued by [redacted] to Mr Philip Farrugia confirming the purchase of an online training course titled [redacted]';

   c. as for the use of laptops, C-Planet clarified that *"[t]he laptops all belong to C-planet and are therefore subject to certain controls* [redacted]. *As a further security*

[33] Supra, section IV.II(b).

measure, [redacted] *This was always the case (even pre GDPR)"*;

d. with reference to the [redacted], C-Planet stated that they [redacted];

e. about the existence of formal policies and procedures, C-Planet pointed out that *"there were no written policies and procedures, but verbal ones were in place and all staff adhered to them. I would like to take the opportunity to include a copy of the written policies that were drafted after the security incident took place* [...][35] *"*;

f. on the matter of secure coding, C-Planet disagreed with the auditor's finding that C-Planet did not follow established secure coding standards to develop and maintain their client's software and business applications. C-Planet explained that [redacted]";

[34] [redacted]

[35] Copies of the policies were attached to the e-mail dated the 4th June 2020 sent to the Commissioner by C-Planet.

g. with regards to the use of dummy data, C-Planet clarified that "[…] *after the security incident took place, a new policy was introduced in order to minimise the risk of a relapse (even though third parties initiated this incident). The policy states that as a general rule, no client data is to ever be present on our development server and only dummy data or randomized data is to be used. The data found on the server REXTESTDEV (the one we supplied* [redacted] *for the investigation by the IDPC) was an exact copy of the server that existed at the time when our systems were hacked. We kept the server "as is" to assist the Police in their investigations following the criminal complaint filed by myself in connection with the said cyber attack* […]*"*;

h. on the use of privacy enhancing technologies such as encryption, obfuscation, pseudonymisation or data minimisation to limit the impact of a privacy breach, C-Planet claimed that, in its view, *"[t]o clarify this point, before the GDPR was introduced there was no legal requirement on how to store data other than general 'security' obligations. Once the stricter rules under the GDPR were introduced, the method of how we developed software changed and this can be checked through the copy of policies attached to this document. As pointed out before, the content of these written policies was already in place (verbally) at C-Planet* […]*";*

i. on the point related to the identified vulnerabilities on the server REXTESDEV, C-Planet made reference "[…] *to the original report(s) we filed with the IDPC where we informed the IDPC that this was originally an internal server that was NOT ACCESSIBLE EXTERNALLY (via a local area network connection). Therefore, these measures were not needed. When the fault in the old server materialised, this data was erroneously included on the server in question that was accessible remotely* […]*";*

j. with reference to the default configuration of index web page of the Apache server, C-Planet did not agree with the statement made by the auditor that reads *"[b]y default web servers are configured to prevent directory listing by showing the default index web page, e.g."index.htlml*". To substantiate its position, C-Planet sustained that *"[t]his statement is incorrect, when apache webservice is setup, it automatically lists all the contents under the folder located at var/www/htlml/* […]*";*

k. C-Planet also disagreed with the auditor's finding that *"[t]he directory listing feature on the Apache web server was enabled in the configuration, and, thus, a listing of the* *directories contained within the document root is automatically shown to the end user due to the missing index file. Therefore, the /va/www/html/_ARCIVE/directory was made easily accessible, allowing the intruder to download files stored inside the web server directory structure including the 'databasebkp.sql' file"*. In its defence, C-Planet contested the use of the phrase "easily accessible" and contended "[…] *to get to that stage the hacker needed more information and not a simply a google search, that is why he used the 'dark Google' searching service SHODAN in order to craft his hacking attack* […]";

l. with reference to the auditor's finding that *"[n]o form of authentication was configured to protect the unauthorised disclosure and eventual misuse of resources stored within the web server directory structure*", C-Planet reiterated that *"[s]ince this data was originally intended only for our internal use, and storage on an internal Lan, these measure were not needed. It was not possible to access that server remotely"*. C-Planet further added that *"[a]n initial remedial measure was made as shown in the report sent to the IDPC, after that, a drastic change to the servers was made in order to minimize the risk of a relapse*";

m. about the auditor's finding that *"[t]he database engine root account was configured with a weak password*", C-Planet commented that *"1. [t]he password was not weak but we concede that it could have been as strong as the other passwords we use (most are checked via* [redacted]*) 2. The reason why the password was not as strong as elsewhere was, once again, because this was a DEVELOPMENT SERVER on a local area network and we already explained how the files in questions were put on the new server in error"*;

n. on the argument sustained by the auditor that the all-powerful root password *"could be leaked from a web server compromise as it is hardcoded in database connection strings inside PHP files pertaining to clients' test software located within the web server document root*", C-Planet rebutted that *"[t]he difference between a development and a production server is largely a matter of security. Typically, a server in a development environment allows unrestricted access to and control by a user or group of users. A production server, on the other hand, is configured to restrict access to authorized users and lo limit control to system administrators* […]. *Once again, I need to emphasize that it is normal in the industry to have this situation (hardcoded credentials in database* *connection strings. Please note that* [redacted] *did not inspect the CLIENT SERVERS we have set up. There, you would see how the issues point out by* [redacted] *do not exist*";

o. as of the auditor's findings on the logs retention period, C-Planet argued that "*[t]he hosting company we use* [redacted] *had imposed this four-week retention policy on us. What is being done right now - until a more long-term solution is found –* [redacted]";

p. as of the auditor's claim that live data, including instances of personal data, were found in the compromised server environment, C-Planet argued that "*[…]* [redacted]";

q. in relation to the regular change of the password for the server 'root' account" C-Planet specified that "*[t]he root account of the server is not generated by C-planet but by the hosting company –* [redacted]*, as we already remarked to* [redacted] *and to the Cybercrime unit when they visited our office. This password would be changed regularly. C-planet would regularly request a reset of password from* [redacted] *(this was a hard policy within C-Planet) and we would work each time with the new password for each connection that was carried out on the server*". In support of this statement, C-Planet submitted a screenshot of logs of regular password resetting;

r. with regard to the auditor's finding that the electoral register data was found in several projects on the development server as it was used as a '*template*' for various software projects for different clients, C-Planet specified that "*[t]he file was 'used' only once as a test for the* [redacted] *The client requested ad-hoc software to be used as part of their 'know your client' procedures (standard in the industry)*". On this point, C-Planet concluded that "*[s]ince we had not been fed any live* *data to work with, we tested the proposed software solution developed by us by 'using' the electoral register at the back end. Client never saw this and in fact, never used or processed this* [...]*";*

s. as of the fact that the auditor established that there were no formal documented IT security and working practices or any checklists to guide C-Planet in delivering services in a consistent and secure fashion, C-Planet commented that "[...] *as IT Security we have a* [redacted] *in place way before the security incident in question where we monitor our clients servers and check for any operating system vulnerabilities and patch the operating system accordingly and assess any anomalies their hardware might experience* [...]*"*;

t. C-Planet disagreed with the auditor's findings that minimal security controls were found on its workstations, that technical security policies were, therefore, decentralised and at each system user's discretion and that standard anti-malware solutions were used without any centralised management to ensure timely signature updates or monitoring and that in addition, no technologies to centralise patch management was used for servers and workstations. In order to sustain its position, C-Planet maintained that *"[o]ur computers (only four in total) are all password-protected as should have been reported by* [redacted] *during the inspection. Computers log out automatically after* [redacted] *minutes at which point the password would need to be re-inserted"*. C-Planet further added that *"[b]efore the security incident we thought and in reality still think that that there is no need for a 'centralised management' system for us because unlike large entities like* [redacted] *itself, we are a micro company and it would be overkill in terms of investment to have such a system in place. Having said that we invested in an opensource solution called* [redacted] *where a centralised endpoint solution was installed with the name of* [redacted] *(after the incident in question)* [...]. *The solution that was being used previously we*[redacted]*, being a cloud based service which performs real-time detection of viruses, malware, etc. But for the sake of moving forward and to adhere to standards set for larger companies we have implanted a system where our 12 servers and 4 workstations are being monitored and checked by ad hoc software (*[redacted]*) and dedicated virtual servers (called* [redacted]*) for added security* [...] *The version of Linux we use releases new versions every April and October. Office practice is* [redacted]

[redacted] […]";

u. concerning the auditor's position about the security implications of the use of [redacted], C-Planet clarified that, in addition to security measures enforced to [redacted], such as requiring a [redacted], it also had in place "[redacted] [redacted] – *Supplied by manufacturer (and imposed on employees but not processed by C-Planet itself)* • [redacted]", which were not reported by the auditor;

v. as for the logs of the server REXTESDEV, which the auditor found to be only available for thirty (30) days as set by the cloud hosting provider, C-Planet pointed out that "*[f]ollowing the incident we tried to manually override this configuration supplied by* [redacted] *and we were unable to do so* […]";

w. in relation to the auditor's claim that "*MySQL general query logs were not enabled, considering that the server was a test/demo environment*", C-Planet rebutted that "*[o]ur developer does not see any benefit in having the logs enabled as this won't help him during his day to day work because if the software is not performing as it should he could check the logs of the APACHE rather than the MYSQL*";

x. in relation to the statement made by the auditor that the REXTESDEV server was configured to expose all required services directly to a public IP address, which implied that the server had no network security infrastructure protecting it from a direct attack, such as by using a firewall, an intrusion detection system, VPN gateway, or some other form of a bastion host, C-Planet reiterated that, as previously declared, "[…] *this is a development machine and certain services are to be running.* [redacted] *a copy of the security setup on the server was handed to IDPC in the report we compiled* […]";

y. in relation to the changes made by C-Planet to its IT environment security posture following the incident, including a [redacted], C-

Planet specified that *"[t]he improvement was carried out is a drastic change for us in financial terms. We see this as an improvement, but it doesn't mean that previously we had nothing in place (ex. operating systems were regularly updated and maintained)* [...]";

z. with reference to the auditor's findings that during an analysis of the data contained in the server REXTESDEV, several instances of the electoral register dataset were found, that two databases on the live MySQL server, *'Elec_Registery'* and [redacted] contained in the identical 330k records that existed on *'databasebkp.sql'*, that a subset thereof of 29k records was found in another database named *'Elect_Registery_*[redacted]' and that the electoral register dataset was found to be accessed by the [redacted] software using a database stored procedure call, allowing for the retrieval of personal details in response to the submission of an ID Card number, C-Planet rebutted that *"[t]he database* [redacted] *drives* [redacted] *software and may therefore be considered as one and the same thingThey contain the same information. The difference between them is that* [redacted] *contains the account section of the program. As stated above, the file 'Elec_Registery' was used only once as a test for the* [redacted] *of the* [redacted]*. The client had requested ad hoc software to be used as part of their 'know your client' procedures (standard in the industry). Since we had not been fed any live data to work with, we tested the proposed software solution developed through the electoral register table*". As of *'Elect_Registry_Distery_*[redacted]', C-Planet maintained that "*this is another project which does not fall under this investigation and the data is different from the data in the file called "Elec_Registery" data. The entries are represented differently, the structure is different as well and there is certainly no '1' or '2' columns as in the other case* [...];

aa. as of the auditor's claim that numerous other SQL script files containing personal data were found in various locations on the server, C-Planet pointed out that *"[b]eing a development server, these file are remnants generated by third party software we use* ([redacted] *ect) for development and as such are found there not by choice"*;

bb. regarding the auditor's findings that personal data were still active within the live MySQL test database and that besides the databases already mentioned, other databases were also found to contain sets of seemingly real personal data, such as *'voters' data'* within the '*votingSystem*' and '*Elec_Registery_*[redacted]' databases, [redacted] [redacted] C-Planet reiterated that "[…] *the data mentioned above is found in the MYSQL server and, as such, it is not accessible to everyone. The tables mentioned above form part of the development of the software to our clients. To our knowledge the MYSQL was not compromised and as such, this data should still be safe.* […] *the files 'votingSystem', 'Elec_Registery_*[redacted]*' as well as* [redacted] *are not related to the matter under investigation and should be treated accordingly. Moreover, just to be clear, I have re-checked the files in question and no columns having '1' or '2' were found - confirming even more that these are completely unrelated to the file provided to me by* [redacted]";

cc. on its previous declaration that the electoral register data "*was used in the past as a 'template' for various software projects to different clients*" and that Philip Farrugia was under the impression that the database was the same dataset that could be acquired from the Electoral Commission, C-Planet claimed that "[…] *My comments referred to the file under investigation - the file "Elec_Registery" provided to me by* [redacted]*. This was the file that I mistook for the Electoral Registry (even due to the name of the file) and which we used ONCE as test data* [redacted]*. This was never used by the client. The other files that may or may not contain 'voter data' are not this file or taken from this file (as best as we can tell). These additional files do not appear to have been compromised and so, they should be outside of the scope of this investigation*";

dd. regarding the fact that when analysing the databases for interoperability or association to the electoral register dataset, the auditor identified that "[redacted] *and* [redacted] *databases do not contain any specific stored procedure with references to the 'Elec_Registery' database or any data set stored within the latter*", C-Planet stated that "*[t]he tables found by the IDPC are for another software we developed for* [redacted] *and the tables there represent the database used by* [redacted] *software which was the old* [redacted] *software before* [redacted] *suite was introduced. There was no need for the file Elec_Registery to be connected to the* [redacted] *and* [redacted] *table even though the file in question was used in connection with specific software designed for* [redacted] […]*. The file in question was given to me by a specific individual who no longer works at* [redacted] […]";

ee. On the auditor's finding that database [redacted] contained a view named *'Full_Details'* that included all fields within the *'Registery'* table in addition to a field *'Age'* auto-calculated via the *'DoB'* field, C-Planet remarked that it was *"[o]nly test data"* which was *"never actually used"*; and

ff. as of the auditor's finding that both [redacted] and *'Elec_Registery'* contained a working stored procedure *'Get_By_IDCard'* which performs a simple look-up by searching through the *'Registery'* table and returns the row of the data that matches the given *'ID Card'* (number) value, C-Planet argued that *"[t]his was test data only [...]"*. On that point, it should be remarked that the procedure *'Get_By_IDCard'* found on the *'Registery'* table prompted an error on the screen when accessed, *"stating it is empty"*.

XIV.III. The auditor's responses

85. On the 26th June 2020, the Commissioner sought the auditor's feedback on C-Planet's comments on the document *'Facts established during the IT Security Audit of C-Planet and the server REXTESTDEV'*. The auditor submitted such feedback to the Commissioner on the 6th July 2020, emphasising that it only responded to C-Planet's arguments which were *"either contradictory or stating incorrect facts"*. The principal arguments made by the auditor are reported hereunder:

a. as for the statement made by C-Planet that *"the server REXTESDEV is a development/test server and was a replacement for the server that was on an internal network"*, the auditor "[...] *acknowledges that a server on an internal network may not require the level of security hardening that a server accessible on the internet, however, REXTESDEV was in fact accessible over the Internet and although it was a test server, it contained real PII* [personal identifiable information]*"*;

b. on the topic of secure coding and on the use of the tool [redacted], the auditor affirmed that *"[w]hile we have acknowledged the use of* [redacted] *as a good practice, the* [redacted] *available within* [redacted] *is not a replacement to the adoption of secure coding standards and practices, such as those established by OWASP* [Open Web Application Security Project]. [redacted]

[redacted]

Furthermore, the official documentation recommends the use of 'prepared statement' to mitigate such vulnerabilities, which falls within the scope of what is referred to as secure coding practice. From our general observations, we did not identify the use of such [redacted]*, neither the use* [redacted]*";*

c. the auditor understood that C-Planet's statement that *"dummy data or altered data is used during development* [...]*"* meant that *"this had been the practice even before the incident"*. Nevertheless, the auditor reiterated that, from its audit findings, *"it seems that PF meant that the policy was introduced after the incident. PF confirms that live data including several sets of personal data, was indeed found to be used on REXTESDEV";*

d. the auditor pointed out that it *"did not intend to imply that C-Planet does not apply any privacy enhancing technologies, but that we found multiple cases of the absence of basic measures that could have prevented the data breach* [...]*";*

e. concerning C-Planet's comments on the auditor's position on the Apache web server default index page, the auditor held that *"C-Planet are stating that when "Apache web service is set up, it automatically lists all the contents under the folder located at /var/www/html/". This is only true if there is no index file (e.g. index.html) in the DocumentRoot directory. Upon installation, a default page is created and placed within this directory and served to the web users* [...]. *If a default or custom index file is missing, the server will list the directory contents. The latter behaviour can also be disabled via the server configuration but was not* [...]*";*

f. regarding C-Planet's argument about the easy accessibility of the html/_ARCIVE/directory, the auditor commented that *"'[e]asily accessible' relates to the ease of access to the directory content once the server was discovered. Security by obscurity is no security at all. All public IP addresses are easily found via open source intelligence tools, and there are both good and bad crawling engines looking for exposed services running behind open ports on these IP addresses"*;

g. on the database engine 'root' account password, the auditor rebutted C-Planet's comments by arguing that *"the database engine 'root' account password was actually weak. It was set to "passwordxxx", with "xxx" being numeric characters at the end. Although we acknowledge this was a development server, may we stress the fact that the MySQL service was publicly exposed on the server's public IP address with real PII data. Further to this, C-Planet was using the root password for all web applications, instead of using a low privileged service account for connection strings on each web application"*;

h. as of C-Planet's statement that *"the difference between a development server and a production server is largely a matter of security"*, the auditor argued that it *"would be acceptable if the data used with the test environment is dummy data. However, basic security practices should still be employed in a development environment to protect other information assets, such as intellectual property. Furthermore, the statement "I need to emphasize that it is normal in the industry to have…(hardcoded credentials in database connection strings)" contradicts good secure coding practices. While this may or may not be a normal practice, it is still a security issue that can be exploited if other security practices are weak. Credentials should be stored in a separate configuration file with restricted permissions and placed outside the web server DocumentRoot so that they cannot be accessed by the exploitation of a web server vulnerability. The PHP connection string can then reference the credentials from that file accordingly.";*

i. regarding C-Planet's additions on the use of screen lockout and password protection to access the workstations, the auditor commented that these were *"good practices but minimal security controls. Centralised management brings is the consistent enforcement of good practices rather than relying on each device user's discretion to always follow policy";*

j. as of MySQL general query logs, the auditor commented that these were *"not used for troubleshooting purposes, but for auditing the SQL queries run against a particular database* […]*"*. The auditor also commented that C-Planet's statement that *"Apache logs instead of MySQL if the software is not working well"* was not logically or technically sound as the two logs recorded different types of activity. The auditor further added that *"[t]he software has both an application and database components, if either of them is* *misbehaving, the respective logs must be checked. It is understood that when troubleshooting an issue with a web application, the developer would generally first examine the web server (Apache) logs*";

k. as for the configuration of the server REXTESTDEV to expose all required service, the auditor argued that "*[t]he necessary precautions should still be taken for a development machine. While it is okay to run all the required services, security hardening means implementing measures to reduce the attack surface. For instance, it is hard to justify why the MySQL service was required to be publicly exposed when this was only required to be accessed locally by the web service running on the same machine";*

l. as for C-Planet's statement *that "[o]ne has to note that the server withstood all the hacking attempts carried out through the SSH and MySQL"*, the auditor commented that *"[t]his is technically not known unless a security analyst has been monitoring the logs generated over the course of time. We have only observed 3-4 weeks' worth of logs";*

m. with regard to the use of [redacted], the auditor elaborated that its understanding was that it "*was one of the measures implemented after the data breach*". The auditor underlined that, when asked whether it used any security measures for detecting intentional/malicious escalation of privileges, C-Planet answered that "*before the breach this was not done, but following the breach various measures have been implemented,* [redacted]". On that point, the auditor concluded that "*we do not exclude our misinterpretation of PF's answer and that* [redacted] *was already in place*";

n. as of C-Planet's statement on the '*Elec_Registery_*[redacted]' database, the auditor sustained that *"[t]he data within this database is not different, is simply a subset of PII data from the 'Elec_Registery' database with a similar but not identical structure – the fields contained in this databases are documented in the report for reference* [...]*";*

o. concerning the various SQL script files identified within the web server, the auditor held that those "*are clearly database dumps/exports. Although we do not rule out that they may have been generated by third-party software, C-Planet could have moved them to a more secure location*"; and

p. with regard to personal data still active within the live MySQL, the auditor observed that *"[w]hile the live MySQL database server was "not accessible to everyone", the lack of security hardening around it (weak passwords, public exposed service, etc.) meant this data could have been compromised before remedial measures were introduced after the incident, without C-Planet's knowledge"*.

XV. LEGAL ANALYSIS AND DECISION

XV.I. C-Planet's role in relation to the processing activity

86. As a preliminary step of this legal analysis, the Commissioner sought, in essence, to establish whether C-Planet was acting in its role as the controller or as the processor in relation to the processing of the personal data contained in the database file, at the time of the incident.

87. The Commissioner emphasised that the concept of controller and its interaction with the concept of processor is crucial to determine who shall be responsible for compliance with the provisions of the Regulation. Although the accountability principle is not new in the data protection legislation framework[36], it has been formalised by the introduction of 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.

88. 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. Notwithstanding the fact that a processor does not process personal data on its own volition but rather on behalf of the controller, the Regulation still imposes several direct obligations upon the processor and therefore, it is essential to clearly outline the roles of the actors involved in the processing activity.

[36] Article 29 Data Protection Working Party, *Opinion 3/2020 on the principle of accountability*, 00062/10/EN, WP173, page 6.

89. The Regulation, which started applying on the 25th May 2018, inherited the definitions of the *"controller"* and the *"processor"* directly from Directive 95/46/EC[37] and therefore, the applicable criteria on how to attribute the roles of the controller and the processor remain substantially the same[38].

90. 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*".

91. 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. The assessment as to whether such influence is exercised or otherwise in a specific case, largely depends on the outcome of the analysis of the circumstances surrounding the processing. Therefore, the question "*who determines the purposes and means of the processing of personal data*" is essential to distinguish between the roles of the controller and the processor.

92. In certain instances, a legal act may appoint a natural or legal person, public authority, agency or other body to act as the controller with respect to one or more specific processing activities. It is also possible that a legal act establishes a task or imposes a duty on someone to collect and process certain data. In such cases, the designation of the controller derives either directly, or else indirectly from the applicable legal provisions.

93. In absence of control arising from legal provisions, the qualification of a party as the controller who is exercising a determinative influence, is established upon the careful assessment of the circumstances surrounding the processing. This is naturally in line with the functional nature of

[37] In Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, the concepts of *"controller"* and *"processor"* were defined respectively in article 2(d) and in article 2(e).
[38] Opinion of Advocate General Bobek of 19 December 2018, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, C-40/17, EU:C:2018:1039, para. 87.

the concept of controller, which is not defined solely by considering legal formalities, but also factual conditions, which are necessary to infer who is exercising a decision-making role in relation to the purposes and means of the processing activity. Indeed, the Court of Justice of the European Union ("**CJEU**") in its settled jurisprudence[39] interpreted the concept of controller in a pragmatic and functional fashion as averse to a purely formal analysis. In doing so, the Court examined thoroughly the factual influence that actors had over the respective processing activities.

94. In this regard, in its Guidelines on the concepts of controller and processor in the GDPR, the European Data Protection Board 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"*[40].

95. A corollary of this "factual" approach is that the attribution of the role of controller is based on who is effectively and concretely making decisions in relation to the purposes and means of a specific processing activity. This is notwithstanding the legal capacity to make such decisions. Therefore, the natural or legal person, public authority, agency or other body which is not legally entitled to make decisions on the purposes and means of the processing of personal data but still does that, shall assume the role as the controller[41].

96. 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

[39] Judgement of the Court (Grand Chamber) of 13 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 5 June 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH,* C-210/16, ECLI:EU:C:2018:388.

[40] European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0 ("**EDPB 07/2020**"), pages 11 and 19.

[41] Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, 00264/10/EN, WP169 ("**WP169**"), page 9.

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.

97. Understanding the role of the processor is equally important to correctly allocate responsibilities in terms of the provisions of the Regulation. Within this context, the Commissioner examined article 4(8) of the Regulation, which defines the role of a processor as *"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". Condicio sine qua non* to qualify as a processor is to process personal data on behalf of the controller. The decisive factor for distinguishing a processor from the controller is that a processor should not process personal data in its own interest and for the purpose of fulfilling its own objectives, but should rather act on behalf of the controller on documented instructions. A processor therefore serves the interests of the controller and it is strictly bound by its instructions, having no or only very little room for making autonomous decisions and acting as an extended arm of the controller.

98. In this context, article 28(3) of the Regulation imposes that the relationship between the controller and the processor shall be formalised by means of *"a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller"*. The Regulation specifies that such legal instrument shall contain certain elements under pain of nullity, one of which is the requirement that a processor, processes the personal data **only on documented instructions of the controller** [emphasis has been added].

99. Whilst decisions about the purposes and means of the processing are essentially made by the controller, however a processor who uses personal data received as a processor beyond the instructions of the controller for its own purposes and determines the means for the processing, shall be considered as the controller in respect of that processing. In this regard, article 28(10) of the Regulation stipulates that "[…] ***if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing*** *"* [emphasis has been added].

100. In the case subject of analysis, C-Planet reiterated in its submissions that it did not act as the controller in respect of the processing of personal data contained in the database file, but rather as a processor engaged by the third party company acting as the controller. For this purpose, the Commissioner proceeded to conduct a thorough exercise to determine, whether C-Planet fulfilled

the role of a processor at the time of the incident, by taking into account the elements collected during the course of the investigation, particularly the factual circumstances of the processing.

101. After carefully examining all the submissions collected during the course of the investigation, the Commissioner noted that both C-Planet and the third party company confirmed that indeed C-Planet had provided certain IT services to the third party company. However, the positions of both companies diverged in relation to the processing operations conducted on the personal data contained in the database file stored on the compromised server. Whereas C-Planet held that the third party company provided the database *"in order to harmonize his data when we were given the task of creating new software for his company*", however the third party company categorically denied this statement, claiming that it had no connection whatsoever with such personal data undergoing processing.

102. Considering that the third party company could not find a signed copy of the agreement between the parties[42], the Commissioner requested additional details to clearly understand the business relationship between both parties. In its response, the third party company sustained that the IT projects for which it engaged C-Planet, had no connection whatsoever with the *"data on about 328,644 voters, including their voting leaning"*.

103. Taking into account the minimum requirements at law to qualify as a processor and given due regard to the formal and factual circumstances of the case, the Commissioner established that a business relationship between C-Planet and the third party company for the provision of IT services existed at the time of the incident. Nevertheless, when restricting the scope of the exercise to the processing activity, which is the subject of this investigation, the Commissioner reached the following conclusions:

   a. that no decision taken by the third party company could be traced, in the sense of delegating the processing activity carried out on the database file to a separate entity (C-Planet), neither from a formal perspective nor from an analysis of the factual circumstances surrounding the processing;

[42] Supra, para. 29.

b. that the evidence gathered does not demonstrate that C-Planet was carrying out data processing activities on the database file to serve the third party company's interests or benefits. As part of the audit, the Commissioner entrusted the auditor to assess whether there was any possible link between the IT systems of C-Planet and the third party company, or any other possible indicator that the source of the file *'databasebkp.sql'* pertained to them[43]. As a result of the analysis of all the databases found on the compromised server, the auditor reported that the database files [redacted] and [redacted] did not contain any specific stored procedure with reference to the *'Elec_Registery'* database or any dataset stored within the latter. Hence, the Commissioner could not ascertain such alleged connection; and

c. that C-Planet failed to provide any concrete evidence, despite being specifically requested to do so, that the third party company provided any documented instructions[44] concerning the processing activity, subject to this investigation.

104. As the next step, the Commissioner proceeded to carry out a test to determine whether C-Planet was acting as the controller whilst processing the personal data contained in the database file at the time of the incident, particularly by assessing the factual circumstances surrounding the processing operation at stake.

105. From the examination of the circumstances, the Commissioner noted that the database file was '*stored*' on a server belonging to C-Planet. By '*storing*' a file that contained personal data, C-Planet was not only '*processing*'[45] the personal data contained therein, but it had *'decided'* the purpose of such processing activity. In fact, during the course of the investigation, the auditor requested C-Planet to clearly explain why the database file was found in several projects on the compromised server. In reply, **C-Planet explained that such file was used in the past as a '*template*' for various software projects developed for different clients**[46] [emphasis has been added].

[43] Supra, para 9(e).

[44] Article 28(3) of the Regulation stipulates that "[p]*rocessing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller* [...]. *That contract or other legal act shall stipulate, in particular, that the processor: (a)* ***processes the personal data only on documented instructions from the controller*** [...]" [emphasis has been added].

[45] Infra, para. 115.

[46] Supra, para. 24 and 81(j).

106. Accordingly, the Commissioner assessed the submissions provided by C-Planet, particularly its declaration, whereby it confirmed that it used a set of personal data supplied by a client to develop projects for other clients. This unequivocally demonstrates that C-Planet had determined the purpose of the processing of the personal data found in the database file on the compromised server[47].

107. As far as the means of the processing are concerned, an intrinsic correlation between the means and the purposes of the processing may be drawn. The '*means*' are nothing but the technical and organisational setting in place to attain the defined purpose of processing. At the time of the incident, C-Planet was processing the personal data contained in the database file for its own benefits and interests, and with its own means, defining *inter alia*, which personal data are to be processed, who had access to the data, and determining the technical and organisational measures to be applied to the processing activity at stake.

108. Accordingly, the Commissioner concluded that at the time of the incident, C-Planet (hereinafter referred to as the "**controller**") had determined the means and purposes of the processing of the personal data contained in the database file, and thus acted as the controller within the meaning of article 4(7) of the Regulation.

XV.II. Lawfulness of the processing

XV.II.I. General Considerations

109. The Commissioner emphasises that the protection of natural persons in relation to the processing of personal data is a fundamental right recognised by article 8 of the Charter of Fundamental Rights of the European Union. The content and structure of article 8 of the Charter helps to understand the constitutive elements of this fundamental right.

110. The first paragraph in a very broad manner provides that *"[e]veryone has the right to the protection of personal data concerning him or her"*. The second paragraph specifies the content of such right by elucidating that *"[s]uch data must be processed fairly for specified purposes and on the basis of consent of the person concerned or some other legitimate basis laid down by law"*.

[47] In EDPB 07/2020, page 26, the European Data Protection Board provided an example of an analogous scenario.

Finally, the third paragraph mandates that *"[c]ompliance with these rules shall be subject to control by an independent authority"*.

111. Accordingly, the provisions of the Regulation aim at protecting fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data. The Commissioner has taken into account this ultimate objective of the Regulation when interpreting and enforcing the law for the purpose of this legal analysis.

112. As a preliminary step of the investigation, the Commissioner examined the following data elements, which were contained in the database file: (i) name and surname; (ii) identity card number; (iii) postal address; (iv) date of birth; (v) data subject's ballot box number; (vi) voting document number; (vii) district; (viii) phone number; (ix) sex; and (x) numerical identifier from 1 to 4.

113. The definition of *'personal data'* as held in article 4(1) of the Regulation provides that *"**any information relating to an identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"* [emphasis has been added].

114. The name and surname of a person[48] combined with a unique identity card number are indeed the most common identifiers to ascertain the identity of the data subject. In this regard, the Commissioner established that all the information contained in the database relate directly to identified natural persons, in the meaning of article 4(1) of the Regulation.

115. In addition, the Commissioner assessed article 4(2) of the Regulation which defines *'processing'* as *"**any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means**, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by*

[48] "[…] *the name of the person is indeed the most common identifier, and, in practice, the notion of "identified person" implies most often a reference to the person's name*", in Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 01248/07/EN, WP136, page 13.

transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" [emphasis has been added].

116. The Commissioner observed that the controller's submissions provide that the database was *"originally intended only for our internal use, and storage on an internal server Lan"* and that such database was used in the past as a '*template*' for various software projects developed for different clients. This is therefore indicative that there was processing of personal data within the meaning of article 4(2) of the Regulation.

117. For the purpose of this analysis, the Commissioner organised the data into three (3) groups: (i) the data which is made publicly available: (ii) the data which is not made publicly available; and (iii) the numerical identifier from '1' to '4'.

118. The principle of fair and lawful processing in terms of article 5(1)(a) of the Regulation, which is one of the data protection principles that constitutes the *'essence'* of the fundamental right to data protection, requires *inter alia* that every data processing operation has a lawful ground for processing. In this regard, article 6(1) of the Regulation stipulates what may constitute such a legal basis, taking also into consideration all the other core principles for processing personal data as set out in article 5 of the Regulation.

XV.II.II. Personal data which is publicly available

119. The Commissioner noted that some of the identifiers which were disclosed, seemed to be the data which is generally contained in the Electoral Register. Consequently, the Commissioner proceeded to investigate this matter by holding a consultation meeting with the Chief Electoral Commissioner[49], during which a matching exercise was conducted to check and verify whether the data extracted from the data file elevated by the Commissioner contain the same data stored by the Electoral Commission on its computer systems.

120. Within this context, the Commissioner assessed article 33(1) of the General Elections Act (Cap. 354 of the Laws of Malta), which establishes that the Electoral Commission "***shall cause a revised Electoral Register to be published in a non-searchable electronic format on its website***

[49] Supra, section IX.

twice a year**, that is to say, in the month of April and in the month of October*" [emphasis has been added]. The scope of such publication is further explained in article 30(3) of the Act, which provides that the "*Electoral Register shall be compiled in such a manner **that the public may be aware of the persons who are registered as voters, and in such manner to enable identification of every voter and giving every voter the opportunity to object to the inclusion of any other voter in accordance with the provisions of this Act." [emphasis has been added].

121. In this regard, article 31(3) of the Act states that "*the Electoral Register may also include against the name of each voter any other particulars which may be considered necessary for the proper identification of each voter*". The Electoral Register contains the following personal data: (i) name and surname of the eligible voter; (ii) address; and (iii) identity card number.

122. Following the matching exercise carried out to verify whether the data contained in the controller's database are indeed the data which have been derived from the Electoral Register, the Electoral Commission confirmed that the "*data* [contained in the compromised database] *included ID card numbers ending with an 'A', it was concluded that **the data pertained to both 2013 Local Councils' elections and 2013 General Elections held on the same day: 9th March 2013***" [emphasis has been added].

123. The Commissioner emphasised that any personal data which are made publicly available shall not give the automatic, absolute right to any controller to process that personal data for a different purpose without a proper legal basis in terms of article 6(1) of the Regulation[50]. This interpretation derives from the purpose-limitation principle as held in article 5(1)(b) of the Regulation, which is one of the fundamental legal precepts entrenched in data protection law and which is prerequisite for most other fundamental requirements in order to ensure legal certainty and predictability.

[50] "*Publicly available data are still personal data subject to data protection requirements, including compliance with Article 7, irrespective whether or not they are sensitive data*", in Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 844/14/EN WP 217, footnote 31, page 15.

XV.II.III. Personal Data which is not publicly available

124. The second group of personal data relates to the data subjects' ballot box number, voting document number, district, date of birth, phone number and sex.

125. In this respect, the Commissioner examined article 64(1)(b) of the General Elections Act, which states that at least fifteen (15) days prior to the day of the election, the Commission shall forward to all the political parties the lists of voters, which lists *"shall identify the polling booth where each voter entitled to vote shall exercise his right to vote, shall list the voters who are to vote in each polling booth in alphabetical order according to the surnames of the voters, assigning to each voter a distinct and consecutive number and indicating the name, surname, address and a legally valid identification document number of each voter as well as the registered number of the respective voting document of each voter"*. It therefore follows that these lists are only made available to the political parties.

126. Within this context, the Commissioner assessed the information which was provided by the Electoral Commission during the course of the investigation, particularly that the "*Commission also confirm that its computer system does not hold* ***other data such as telephone number of voters and therefore no such data was provided by the Commission to the party delegates mentioned above***" [emphasis has been added].

XV.II.IV. Special Categories of Personal Data

127. Finally, the Commissioner noted that the third group of data consists of another data category which is not processed by the Electoral Commission. The database contains a numerical identifier from 1 to 4, which the media alluded that it refers to the data subjects' political opinions. After assessing the nature of the personal data and the context within which such data are processed, the Commissioner concluded that the numerical identifier, combined with the other data, particularly the voting document number and the ballot box number, is referring to the political opinions of the affected data subjects.

128. The Regulation provides heightened protection to the processing of special categories of personal data due to the significant risks in relation to the protection of the data subjects' rights and freedoms, particularly the irreversible and long-term consequences, which may occur as a result

of the processing activity[51]. In fact, in the ruling *GC and Others v Commission nationale de l'informatique et des libertés* (CNIL), the CJEU stated that article 9(1) of the Regulation provides "*enhanced protection as regards such processing, which, because of the particular sensitivity of the data, is liable to constitute, as also follows from recital 33 of that directive and recital 51 of that regulation, **a particularly serious interference with the fundamental rights to privacy and the protection of personal data, guaranteed by Articles 7 and 8 of the Charter**.*"[52] [emphasis has been added].

129. In its Guidelines on Personal Data Breach Notification under Regulation 2016/679 issued by the Article 29 Working Party (the "**WP29**") and endorsed by the European Data Protection Board, the expert group highlighted that any breach which involves the disclosure of political opinions to unauthorised third parties presents an intrinsic high risk to those individuals, whose data have been unlawfully processed[53].

130. The Commissioner established that the processing of personal data revealing political opinions are special categories of personal data in terms of article 9(1) of the Regulation. In this regard, the European Court of Human Rights considered "*that personal data revealing political opinion falls among the special categories of sensitive data attracting a heightened level of protection*"[54].

131. For this purpose, the Commissioner examined the wording of article 9(1) of the Regulation, which, as a general rule, prohibits the "***[p]rocessing of personal data revealing** racial or ethnic origin, **political opinions**, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*" [emphasis has been added]. The specific prohibition set out in article 9(1) of the Regulation is not triggered insofar as one of the statutory exceptions laid down in article 9(2) of the Regulation applies.

[51] Recital 51 of the Regulation: "*Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms.*"

[52] Judgment of the Court (Grand Chamber) of 24 September 2019, *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)*, C-136/17, para. 44.

[53] Article 29 Data Protection Working Party, *Guidelines on Personal data breach notification under Regulation 2016/679*, 18/EN, WP250 rev.01 ("**WP250**"), page 23.

[54] ECtHR, *Catt vs the United Kingdom*, no. 43514/15, delivered on the 24th January 2019.

132. Therefore, a controller processing special categories of personal data cannot invoke solely a legal ground in terms of article 6(1) of the Regulation, but it shall also ensure that one of the exceptions listed in article 9(2) applies. Recital 51 of the Regulation clarifies that, in addition to the specific requirements for the processing of special categories of personal data, the general principles and other provisions of the Regulation shall apply, *"in particular as regards the conditions for lawful processing"*. It therefore follows that article 6(1) and article 9(2) shall apply in a cumulative manner and, in the absence of this, the processing shall be deemed to be unlawful.

133. In view of the foregoing, the controller infringed article 6(1) of the Regulation for having processed personal data without any valid lawful bases. Additionally, the controller infringed article 9(1) of the Regulation for having processed personal data revealing political opinions, where none of the exemptions of article 9(2) of the Regulation could apply.

XV.III. The obligation to provide information to the data subjects

134. 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"*.

135. 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[55], 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[56], 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*

[55] Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679*, 17/EN, WP260 rev.01 (**"WP260"**).

[56] Judgment of the Court (Third Chamber) of 1 October 2015, *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others*, C-201/14, ECLI:EU:C:2015:638, para. 33.

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".

136. 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"*[57] [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].

137. Article 14 of the Regulation places an obligation upon the controller to provide the data subject with details about the processing activity where the personal data have not been obtained directly from him or her. The fact that the Regulation distinguishes between direct and indirect collection of personal data is indicative that the transparency and fairness principle should also apply to those cases where there is no direct contact between the controller and the data subject at data collection stage.

138. The wording used by the legislator in article 14(1) of the Regulation, specifically the verb "*shall provide*" demonstrates that the controller has the obligation to proactively provide the information concerning the processing activity and the wording used does not leave room for optional disclosures, unless the controller can effectively demonstrate that one of the exemptions listed in article 14(5) applies.

139. The Commissioner stresses the importance of article 14 of the Regulation specifically because the personal data is not provided by the data subject, but obtained from third party sources. In this regard, the controller is obliged to inform the data subjects of the details of the processing activities in the manner prescribed by the Regulation, which is a *sine qua non* for ensuring transparency, fairness and enabling the data subject to exercise control over their personal data.

[57] WP260, page 5.

140. Article 14(1) and (2) prescribes the list of information that shall be provided to the data subject. Even though the legislator distinguishes between the two sets of information, however, it is abundantly clear that all such information should be provided to the data subjects. In addition to the information which the controller is obliged to provide in terms of article 13 of the Regulation, the legislator included two (2) other types of information: (i) the categories of personal data concerned and (ii) the source from which the personal data originates.

141. The data subjects should have a precise description of the categories of personal data processed about them, especially because the personal data have not been obtained from the data subjects, who therefore lack awareness of which categories of personal data are processed[58]. Additionally, the Regulation obliges the controller to disclose the specific source of the personal data and whether it came from publicly available sources.

142. As a general rule, article 14(3)(a) of the Regulation imposes an obligation upon the controller to provide information within a reasonable period after obtaining the personal data, but at least within one (1) month after having obtained it.

143. Having considered that, notwithstanding the fact that article 5(1)(a) of the Regulation encompasses the principle of lawfulness, transparency and fairness, the Article 29 Working Party[59] emphasises that *"[t]he requirement for transparency* ***exists entirely independently of the requirement upon data controllers to ensure that there is an appropriate legal basis for the processing under Article 6****"* [emphasis has been added].

144. In the present case, the controller had not obtained the personal data concerning the affected data subjects directly from them, but rather from a third party which could not be determined during the course of the investigation. As a consequence, the controller should have informed the data subjects pursuant to article 14 of the Regulation within the statutory deadline stipulated therein.

145. From the findings of the investigation, the Commissioner concluded that the controller did not inform the affected data subjects in the manner prescribed by the Regulation, thus infringing article 14 thereof.

[58] Ibid., page 36.
[59] Ibid., page 9.

XV.IV. The delay in the notification and the lack of communication of the personal data breach to the affected data subjects

146. Article 33 of the Regulation binds the controller to notify the supervisory authority a personal data breach which is likely to result in a risk to the rights and freedoms of natural persons, by no later than seventy-two (72) hours after becoming aware of it. In case the notification is not made within seventy-two (72) hours, the controller shall provide reasons for the delay.

147. On the other hand, article 34 of the Regulation lays down the obligation to communicate a breach to the affected data subjects. Article 34 requires a higher threshold for communicating the data breach, in fact the wording of the law specifies that "*[w]hen the personal data breach* ***is likely to result in a high risk*** *to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay*" [emphasis has been added].

148. Upon encountering a personal data breach, the controller should not only act to maintain the potential prejudicial consequences of such an incident, but also assess the level of risk that the breach is likely to pose in order to define which actions need to be taken according to its breach reporting obligations.

149. The Commissioner examined the complete notification submitted on the 1st April 2020, wherein the controller marked the severity of the potential impact of the breach as *'high'* and recognised that such incident might have negative consequences upon the data subjects, specifically, by describing the likely consequences of the breach as follows: "*loss of control over personal data*" and "*inappropriate usage of contact details*".

150. For the purpose of this analysis, the Commissioner carried out an assessment based on the hereunder factors which according to the WP29[60] are necessary to determine the severity of the potential impact upon the affected data subjects and consequently, the associated level of risk. This assessment is indeed essential to enable the Commissioner to establish whether the actions taken by the controller following the breach were in line with the requirements of the Regulation.

[60] WP250, pages 20 – 22.

XV.IV.I. The type of breach

151. The personal data breach encountered by the controller is a confidentiality breach, which resulted in the disclosure of personal data to unauthorised recipients. The nature of the personal data at stake – which also includes a special category of personal data – adds to the gravity of the incident.

XV.IV.II. The nature, sensitivity, and volume of personal data

152. As outlined hereabove[61], the personal data which were disclosed to unauthorised recipients, contained several identifiers which when combined together could be *"typically more sensitive than a single piece of personal data"*[62].

153. Furthermore, special categories of personal data are, by definition, sensitive. In this regard, the WP29's position is that *"[u]sually, the more sensitive the data, the higher the risk of harm will be to the people affected"*[63].

154. In evaluating the appropriateness of the technical and organisational measures vis-à-vis the risk posed by the processing[64], the Commissioner examined the volume of the personal data, which was undergoing processing by the controller at the time of the incident. Given that the controller was processing several categories of personal data linked to a large number of data subjects, the volume of the personal data was significant. In this regard, the WP29's position clarifies that *"a breach affecting large volumes of personal data about many data subjects can have an effect on a corresponding large number of individuals"*[65].

XV.IV.III. Ease of identification of individuals

155. In determining the ease of identifying the data subjects, the Commissioner noted that the controller processed several identifiers which when combined together, made the identification of the data subjects possible without the need to conduct any further research to discover their

[61] Supra, section XV.II.
[62] WP250, page 24.
[63] Ibid.
[64] Infra, section XV.V.
[65] WP250, page 24.

identity. Besides, it should be remarked that the technical and organisational measures implemented by the controller did not include, for example, pseudonymisation and encryption, which techniques render the personal data unintelligible to unauthorised recipients, in case of a personal data breach.

XV.IV.IV. Severity of the consequences for the affected data subjects

156. The severity of the consequences of a personal data breach upon the data subjects largely depends upon the nature of the personal data affected by the breach. The involvement of special categories of personal data is an indicator that the impact on data subjects can be especially severe[66].

157. Given that the controller processed a substantial amount of personal data, including *inter alia* data revealing the political opinions of a large number of data subjects, the processing activity was likely to pose a high risk to the rights and freedoms of the data subjects.

XV.IV.V. The number of affected data subjects

158. Considering that *"[g]enerally, the higher the number of individuals affected, the greater the impact of a breach can have"*, the Commissioner had given due regard to the fact that three hundred thirty-seven thousand and three hundred eighty-four (337,384) data subjects were affected as a result of the personal data breach, as further elaborated in the sections hereunder[67].

XV.IV.VI. Personal data breach resulting in a high risk to the rights and freedoms of natural persons

159. Having objectively examined the factors listed above, the Commissioner determined that the potential impact of the breach upon the affected data subjects is severe. In light of this, the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, as in fact, indicated by the controller in its complete notification submitted on the 1st April 2020.

160. Hence, it resulted that the controller should have:

[66] Ibid.

[67] Infra, section XV.V.II.

a. notified the breach to this Office by not later than seventy-two (72) hours after becoming aware of the breach; and

b. communicated the breach to the data subjects without undue delay.

XV.IV.VII. The obligation to notify the supervisory authority

161. On the 1st April 2020, the controller notified the breach to this Office, indicating the 29th February 2020 as the date of the breach and the 31st March 2020 as the date of awareness of the breach.

162. In the same notification, the controller further explained that *"[t]he discrepancy between the date of breach and awar[e]ness is due to someone sent a tweet informing me that there is a breach but I did not take notice as I use twitter sporiadically. In the meantime we noticed that the server was not performing as it should be and we carried out maintenance on it, thus removing the file when we realized it was on the server*".

163. Conversely, in both the preliminary and complete technical reports, the controller confirmed that it had indeed received an e-mail from an individual on the 29th February 2020[68] *"stating that we had a hole in our server and that we should fix it and attached two screenshots"*. The controller contended that it *"took this information to heart **and investigated the issue on the server"***, after which ***"[t]he directory listing was locked by a username and password, and a plan was set in motion to lock the server even more. The username and password were in place by the 5th March 2020, not as indicated in the media, and a plan was also initialized to increase the security on the connections to the server and to remove the_ARCHIVE folder from the server"*** [emphasis has been added].

164. In its two-fold notification to this Office, the controller erroneously declared that the date of awareness of the breach was the 31st March 2020. From further investigations, it emerged that by the 5th March 2020, the controller was fully aware of the incident, however, it was only on the 1st April 2020, that the controller took action by notifying the breach to the Commissioner, without providing any valid reasons for the delay.

[68] According to the WP29 (WP250, page 11), the awareness requirement may be fulfilled by information given *by an individual, a media organisation, or another source*".

165. Having given due regard to the fact that the controller did not notify the Commissioner within seventy-two (72) hours after having become aware of it and failed to provide reasons for the delay, the controller infringed its obligation to report the personal data breach in terms of article 33(1) of the Regulation.

XV.IV.VIII. The obligation to communicate the personal data breach to the data subjects

166. The personal data breach's likeliness to pose a high risk to the rights and freedoms of natural persons triggers the communication obligation vis-à-vis article 34 of the Regulation.

167. Such provision stipulates that in certain instances, notwithstanding the high risk, the communication in question is not required. Accordingly, in its notifications to this Office, the controller indicated that the reasons for not informing the data subjects were due to the fact that *"[i]t would involve disproportionate effort to inform each data subject individually"* and that it had implemented certain measures, which included *"appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it"* and *"measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise"*.

168. Despite the fact that communication is not necessary when any of the conditions set forth in article 34(3) of the Regulation are met, the controller shall be responsible for, and be able to concretely demonstrate how any of these conditions are fulfilled to safeguard the rights and freedoms of the data subjects. In this regard, the WP29 sustained that *"[i]n accordance with the accountability principle controllers should be able to demonstrate to the supervisory authority that they meet one or more of these conditions"*[69].

169. In this regard, the Commissioner examined the controller's position about the communication requirement, particularly the exemptions invoked in terms of article 34(3) for not communicating the breach to the affected data subjects.

[69] WP250, page 22.

170. In relation to the controller's statement that *"[i]t would involve disproportionate effort to inform each data subject individually"*, the Commissioner considered the WP29's position, which provides that, despite the fact that a direct communication to the data subjects is preferable[70], however, pursuant to article 34(3)(c) of the Regulation, the communication requirement may still be fulfilled, by means of a public communication or a similar measure whereby the data subjects are informed in an equally effective manner. Evidently, the controller failed to deliver any such measures, in spite of the fact, that it was in a position to do so.

171. Having assessed the implementation of appropriate technical and organisational protection measures by the controller to the personal data affected by the personal data breach, in particular to render the personal data unintelligible to any person who was not authorised to access it, such as encryption, and the subsequent measures implemented by the controller to ensure that the high risk to the rights and freedoms of data subjects was no longer likely to materialise, the Commissioner determined that indeed, the controller had adopted certain measures to the compromised server following the breach, such as for example, by setting a password. Nevertheless, the application of these measures was not sufficient to impede the high risk to the rights and freedoms of data subjects to materialise, due to the fact that unauthorised access to the server and unlawful disclosure of that personal data contained therein had already occurred.

172. Based on the foregoing considerations, the controller infringed article 34(1) of the Regulation for not having communicated the personal data breach to the data subjects where the conditions of law were fulfilled, and no exemption applied.

XV.V. Technical and organisational measures

173. Article 5(1)(f) of the Regulation lays down the principle of integrity and confidentiality, which establishes that processing shall be carried out in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (the "**security measures**"). By virtue of the principle of accountability set out under article 5(2) of the Regulation, the controller shall be responsible for, and must be able to demonstrate

[70] WP250, page 21.

compliance with the principles of data processing, including the principle of integrity and confidentiality.

174. Such principle is further specified in article 32(1) of the Regulation, which is more prescriptive and sets out the obligations to which, both controllers and processors are subject in terms of data security. According to article 32(1) of the Regulation, controllers and processors shall implement appropriate technical and organisational measures **to ensure a level of security appropriate to the risk**, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Article 32(1) of the Regulation provides a non-exhaustive list of those measures.

175. From the analysis of the relevant legislative framework, it transpires that there is no space for a *'one size fits all'* approach when it comes to selecting security measures to protect the personal data. The security measures should rather be chosen on a bespoke basis, and only after a thorough assessment to ensure that these measures are likely to achieve their objectives, and on weighing competing interests, such as the consequences that such a measure has on an interest worthy of legal protection. This obliges the controller to put into place proactive measures to ensure effective compliance with the data protection legislative framework.

176. The obligation of personal data security should therefore be construed as an obligation to guarantee a *"level of security appropriate to the risk"*. In this aspect, article 32(2) of the Regulation stipulates that *"in assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed"* [...] *"which may in particular lead to physical, material or non-material damage*" (Recital 83 of the Regulation). Recital 76 of the Regulation sheds some light on the nature of such assessment, pointing out that it should be *"objective"* and that its outcome should establish *"whether data processing operations involve a risk or a high risk"*. The same recital indicates that *"[t]he likelihood and severity of the risk to the rights and freedoms of the data subject should be determined* ***by reference to the nature, scope, context and purposes of the processing****"*. [emphasis has been added]. The recurrent concept of risk can be seen in a number of provisions of the Regulation, specifically articles 24, 25, 30 and 35, which provisions impose a number of obligations upon controllers on a risk-approach basis.

177. In one of its guidelines, the European Union Agency for Network and Information Security ("**ENISA**") provides an overview on how an information security risk management process may be adopted to meet the security requirements of the Regulation. According to ENISA, *"[i]n the 'typical' risk assessment process, the risks are estimated based on their potential impacts to the organization.* ***In the case of personal data processing, however, the impacts are considered with regard to the freedoms and rights of individuals****"*[71]. As far as the management of the encountered risks is concerned, ENISA explained that *"the way that the identified risks are managed may also defer from the 'typical' risk assessment process"* and *"the adoption of specific technical and organizational measures might be different between the 'typical' risk management process and the data protection risk management"*[72]. In principle, only after having assessed the risk, the controller or a processor may select security measures that are appropriate to counter the risk and effectively preserve the integrity and confidentiality of the personal data undergoing processing.

178. According to ENISA[73], the impact of a potential personal data breach on the rights and freedoms on the individuals constitutes a major aspect of the above-described risk assessment. In this regard, the WP29 stressed that *"[w]hen considering a potential breach, it looks in general terms at the likelihood of this occurring, and the damage to the data subject that might ensue; in other words, it is an assessment of a hypothetical event"*[74]. The controller should have, therefore, evaluated the risk posed by the potential occurrence of a personal data breach, and on the basis of the outcome of that analysis, it should have implemented appropriate technical and organisational measures to prevent the materialisation of the risks envisaged and to effectively respond, in a timely fashion, to such a breach.

179. Giving due regard to the difference between the risk assessment which the controller has to carry out with the aim of evaluating the risk of unauthorised or unlawful processing and against accidental loss, destruction or damage of the personal data, and the data protection impact assessment exercise, which scope and purpose goes beyond data security, article 35(3) of the Regulation provides some examples of processing activities that inherently present a high risk, thus triggering the data protection impact assessment requirement. The WP29 provides insight

[71] ENISA, *Guidelines for SMEs on the security of personal data processing*, December 2016, section 2(3)(2), page 17.
[72] Ibid.
[73] Ibid., section 2(3)(1), page 13.
[74] WP250, page 23.

on the criteria that have to be considered in order to identify processing operations which are likely to result in a high risk. The following criteria are relevant to the situation at stake, and the Commissioner assessed them against the specific processing activity carried out by the controller.

XV.V.I. Special categories of personal data or data of a highly personal nature

180. In line with the wording of the WP29, a criteria which suggests high risk is processing which *"includes **special categories of data as defined in Article 9 (for example information about individuals' political opinions)**"* [emphasis has been added]. Accordingly, recital 75 of the Regulation provides that *"[t]he risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular:* [...] ***where personal data are processed which reveal*** [...] ***political opinions*** [...]*"*. As elaborated above[75], the controller processed personal data revealing political opinions, which is a special category of personal data under the Regulation, without a valid legal basis. The controller argued that it was *"always under the impression that this was simply the electoral register"* and *"believed it to be the same file one could obtain from the central government"*. However the investigation revealed that such file contained supplementary information when compared to the 2013 version of the electoral register, which information is not made publicly available by the Electoral Commission[76] in terms of its obligation at law.

XV.V.II. Data processed on a large scale

181. Whilst the Regulation does not provide a definition of *'large-scale'*, recital 91 of the Regulation stipulates that a data protection impact assessment should "[...] *in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk* [...]*"*. The WP29 advised that the following criteria should be considered when establishing whether large-scale processing takes place: (a) the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; (b) the volume of data and/or the range of different data items being processed; (c) the duration, or

[75] Supra, para 127 to 133.

[76] Supra, para 36.

permanence, of the data processing activity; and (d) the geographical extent of the processing activity[77]. In the situation at stake, the Commissioner took into consideration that:

a. the database file affected by the incident contained personal data which pertained to a large number of data subjects, which represented nearly the entirety of the 2013 general elections electorate;

b. the volume of the data processed within the database file was substantial, and, due to the combination of biographical details, electoral details and contact details, the affected data subjects were fully identified;

c. considering that it was not possible for the auditor to establish the source of the compromised database file[78], the Commissioner could not establish the date when the data processing activity commenced; and

d. the geographical extent of the processing was extended to cover the majority of the population of Malta.

XV.V.III. Datasets that have been matched or combined

182. According to the WP29, another indicator of high-risk processing is that *"[d]atasets* [...] *have been matched or combined, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject"*. In this regard, the controller declared that the database file was used in the past as a *'template'* for various software projects that the controller developed for different clients. As part of the objectives of the audit, the auditor was specifically tasked to investigate *"[a]ny interoperability between the compromised file containing the compromised database and other systems/servers* [...]". The auditor found that "*the compromised file 'databasebkp.sql'* ***is an old database SQL script file that contains all the***

[77] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 17/EN WP 248 rev.01, page 10.

[78] In the analysis of any interoperability between the file containing the compromised database and other systems/servers (objective E of the audit), the auditor observed that "[t]*he 'databasebkp.sql' is a database dump and there is no trail that could indicate how, where, and from which entity the set of data was sourced*".

necessary information for recreating database schemas and data for various C-Planet clients from 2017 *used in the recovery process following a hardware failure at that time*" [emphasis has been added]. When accessing the Live MySQL test database, the auditor also found that it "*contains numerous database schemas for various clients, some of which also existed within the older backup file 'databasebkp.sql'.* [redacted] ***identified that the 'Elec_Registery',*** [redacted]***, and*** [redacted] ***databases' all contained approximately the same 330k rows of personal information*** [...] ***within a table called 'Registery' (or 'registery') including the same 17 fields, as illustrated below. Furthermore, a database 'Elec_Registery_***[redacted]***' was found to contain a subset of the same data, approximately 29k rows, within a table called*** [redacted] ***with slight variations in the fields, as illustrated below***" [emphasis has been added]. From those findings, it is evident that the controller used the same database schema for different projects, which action resulted in the combination of datasets containing personal data in a manner which exceeded the reasonable expectations of the data subjects.

183. In view of the foregoing, by processing the personal data contained in the compromised server, the controller engaged in an operation that was, pursuant to the WP29's criteria, likely to pose a high risk. Giving due regard to the risk-based nature of the security obligations of the Regulation, the controller should have evaluated the risk that such processing activity could have posed *prior to* commencing the processing activity, and should have taken structured, balanced and targeted measures to manage the envisaged risk.

184. On the other hand, from the contents of the auditor's report, it transpired that the controller did not carry out such an assessment[79], and did not in any manner evaluate the impact of the processing against the freedoms and rights of individuals, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing.

185. Considering that the selection of appropriate measures to safeguard the security of the personal data should follow from an evaluation of the risks to the rights and freedoms of the data subjects, it is materially impossible to manage a risk which it had not previously identified[80]. In this regard,

[79] In the analysis and evaluation of C-Planet's security policies and procedures (objective D of the audit), the auditor found that "[e]*vidence of security and privacy practices were also found to be lacking,* ***such as conducting some form of risk assessments*** *and regular security testing and assessments*" [emphasis has been added].

[80] "[f]*ollowing the evaluation of the risk level, the SME can proceed with the selection of appropriate security measures for the protection of personal data*" in ENISA, *Handbook on Security of Personal Data Processing*, December 2017, para. 2(1)(5), page 16.

the Commissioner established that the technical and organisational measures that the controller implemented to manage the risks were not commensurate with the risk posed by the processing, particularly due to the fact that the controller was unaware of the risk posed by the processing and it could not explain the logic for implementing one specific security measure over another. As a result, the controller did not implement the *"appropriate technical and organisational measures to ensure a level of security appropriate to the risk"* and overlooked certain vulnerabilities[81] - intended as *"weakness*[es] *of an asset that can be exploited by one or more threats"*[82] which eventually led to the materialisation of the personal data breach.

XV.VI. Exercise of corrective powers

186. Having scrutinised the toolkit of corrective powers at the disposal of the Commissioner in its capacity as the 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 prerogative to issue a reprimand to a controller or a processor and the power to impose an administrative fine pursuant to article 83 of the Regulation, in addition to, or instead of other measures, depending on the circumstances of each individual case.

187. As established during the course of the investigation, the controller is responsible for multiple infringements, which touch upon the very core of the Regulation, thus warranting a level of enforcement which a reprimand, a measure intended for less serious violations, cannot attain.

188. 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 letters (a), (b), (c), (d), (f), (g), (h) and (k) thereof, are of relevance to the present case.

[81] Supra, sections XI.II and XI.III.

[82] Definition based on ISO/IEC IS 13335-1 provided in ENISA ad hoc working group on risk assessment and risk management, *Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs)*, Deliverable 2, Final Version 1.0, 30/03/2006, para. 3.1, page 9.

XV.VII. The assessment on the basis of article 83(2) of the Regulation

XV.VII.I Article 83(2)(a) of the Regulation

189. With regard 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*", the Commissioner made the following considerations.

190. The detected infringements form part of two separate, albeit related set of processing activities. The first one is represented by the processing of personal data, including a special category, without a valid legal basis, in relation to which the controller neglected its obligations in terms of transparency and security. Particularly, the inappropriateness of the technical and organisational measures implemented by the controller in comparison with the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, has a direct, consequential link with the second set of processing activities, which resulted in the disclosure of the personal data undergoing processing to unauthorised recipients. Without prejudice to the fact that the processing operation was unlawful, the unauthorised disclosure of personal data could have been easily prevented if the controller had duly defined and put in place the necessary and appropriate security measures.

191. When the incident occurred, the controller did not take steps to assess whether a risk to the rights and freedoms of natural persons was likely to materialise, and subsequently failed to examine the level of risk. Consequently, the controller did not notify the incident to this Office within the period stipulated in article 33(1) of the Regulation, and it did not inform the data subjects about it, which omissions resulted in further infringements.

192. Each of these sets of processing activities, which are naturally interlinked, result in several infringements of the Regulation. Having further considered the underlying controller's negligence leading to these infringements[83], the Commissioner established that article 83(3) of the Regulation applies to the present case.

[83] Infra, section XV.VII.II.

193. According to such provision, in case of multiple infringements, the total amount of the administrative fine should be capped to the amount specified for the gravest infringement. The Commissioner resorted to Article 29 Working Party's guidance[84] to construe the concept of "**gravity**" of an infringement. According to the expert group, it is not only the **nature** of the infringement, loosely translated into a formal classification of offences into sanctionary levels[85], which should be deemed as the determining factor in the assessment of the gravity of the infringement. Other contextual factors, such as the scope, purpose of the processing concerned, as well as the number of affected data subjects, should also be considered.

194. The Commissioner dealt with the **scope** of the processing operation while assessing the appropriateness of the technical and organisational measures vis-a-vis the level of risk posed by the processing[86]. In this regard, the Commissioner found that the large-scale processing operation undertaken by the controller is a risk-increasing factor adding to the gravity of the combined infringements.

195. While conducting an analysis of the circumstances of the processing to determine the role of C-Planet[87], the Commissioner evaluated the **purpose** sought by the controller, specifically that the personal data was used to develop software projects for its clients as part of its commercial activity. The fact that this purpose relates to the core business activity of the controller, to which the processing activity operated *contra legem*, is an indicator that the controller acted negligently.

196. Given that the Article 29 Working Party recommends a relative rather than absolute approach in the definition of the **number of data subjects** affected by the infringements[88], the Commissioner has taken into account that in the present case, such number is substantial when compared with the population of the country[89]. A considerable number of data subjects were indeed affected by the incident as a result of the lack of adequate routines, thus revealing a high degree of negligence by the controller in handling such a large amount of personal data without the necessary and appropriate safeguards.

[84] Article 29 Data Protection Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, 17/EN WP253 ("**WP253**").

[85] "*[a]lmost all of the obligations of the controllers and processors according to the Regulation are categorised according to their nature in the provisions of article 83(4) – (6)*", ibid.

[86] Supra, para. 181.

[87] Supra, para. 106 and 107.

[88] WP253, page 10.

[89] Supra, section XV.IV.V.

197. Having outlined the context of the processing, the Commissioner then moved onto a formal analysis of the **nature** of the infringements. These concern: (i) the unlawfulness of the processing[90] activity and the lack of compliance with the information obligation[91], and (ii) the lack of compliance with data security obligations[92], and with the notification obligations as set forth in articles 33 and 34 of the Regulation[93].

198. The Article 29 Working Party explained that "*[t]he occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement*".

199. The first category of infringements, falling under the sanctionary tier of article 83(5) of the Regulation, which penalises the controller with "*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*", is the more serious between the two groups.

200. On the basis of the foregoing, the maximum of the administrative fine is hereby being computed within the limit established by the aforesaid penalty tier.

XV.VII.II. Article 83(2)(b) of the Regulation

201. WP253 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*[94]".

202. On the basis of the facts gathered during the course of the investigation, the Commissioner established that there is no evidence that the controller had acted intentionally, although its actions and omissions demonstrate serious lack of diligence. Particularly, the investigation and

[90] Supra, section XV.II.
[91] Supra, section XV.III.
[92] Supra, section XV.V.
[93] Supra, section XV.IV.
[94] WP253, page 11.

the technical audit established that the controller caused the incident for not having implemented basic technical and organisational measures, when it was legally bound to do so.

XV.VII.III. Article 83(2)(c) of the Regulation

203. Another relevant factor which is taken into account is article 83(2)(c) of the Regulation, which refers to *"any action taken by the controller or processor to mitigate the damage suffered by data subjects"*. Given that *"[a] personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons"*[95], the controller should react promptly upon the detection of a personal data breach to decide on the actions to be taken. Following a personal data breach, the controller should, by all means possible, impede that any damage to data subjects materialises.

204. From the facts gathered during the investigation, the Commissioner established that the controller was informed about the incident on the 29th February 2020. Notwithstanding this, the controller did not take immediate action thereupon. It was only on the 5th March 2020, after the incident was made public on for the second time, that the controller took some form of action. As a result, the controller did not act promptly to rectify a situation which was likely to pose a risk to the rights and freedoms of the data subjects, and it failed to ensure that the integrity and confidentiality of such personal data were indeed protected. On the contrary, it negligently responded to the incident with a tardive action, thus adding to its degree of responsibility in managing the incident and its ramifications.

XV.VII.IV. Article 83(2)(d) of the Regulation

205. Article 5(2) of the Regulation sets out the principle of accountability, pursuant to which *"[t]he controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1"*, which paragraph in turn enumerates the principles relating to the processing of personal data. In connection with article 5(2) of the Regulation, article 24(1) thereof establishes an out-and-out principle of responsibility according to which *"[t]aking 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, **the controller shall implement appropriate technical and***

[95] Recital 85 of the Regulation.

organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation" [emphasis has been added].

206. The principle of accountability, read in combination with the nature and scope of the responsibility of the controller, is one of the main pillars of the Regulation. Such principle places responsibility upon the controller to take pro-active action to ensure that the personal data processing activities are aligned with the data protection law, and that the same controller is in a position to effectively demonstrate compliance. Accountability is not only a legal principle, but is also a crucial aspect of the fiduciary obligation between the controller and the data subject, which arises from the data subject entrusting the controller with his or her personal data. In this aspect, the Article 29 Working Party held that *"[r]esponsibility and accountability are two sides of the same coin and both essential elements of good governance.* ***Only when responsibility is demonstrated as working effectively in practice can sufficient trust be developed***"[96] [emphasis has been added].

207. Pursuant to article 83(2)(d) of the Regulation, the examination of the appropriateness of the technical and organisational measures implemented by the controller to protect the integrity and confidentiality of the personal data is a substantive component of the exercise of evaluating the degree of responsibility of the controller. Following the notification of the incident by the controller, the Commissioner conducted a comprehensive analysis of the technical and organisational measures, which the controller had implemented at the time of the incident to verify whether the controller *'did what it could be expected to do'* given the nature, purposes and size of the processing, seen in the light of the obligations imposed on it by the Regulation[97].

208. The Commissioner concluded that the processing activity affected by the incident was likely to present a high risk to the rights and freedoms of the data subjects[98], however he ascertained the technical and organisational measures implemented by the controller did not ensure a level of security appropriate to such risk. From the investigation, it emerged that the security measures in place at the time of the incident were not selected following an organic assessment of the risk posed by the processing. Thus, the lack of basic security measures left room for major

[96] WP173, page 7.

[97] WP253, page 13.

[98] Supra, para. 183.

vulnerabilities and led to the materialisation of the incident[99], adding to the degree of responsibility of the controller.

XV.VII.V. Article 83(2)(f) of the Regulation

209. Article 83(2)(f) of the Regulation provides that the degree of cooperation with the supervisory authority should be taken into consideration when deciding whether to impose an administrative fine and the amount of the fine.

210. The Commissioner acknowledges that the controller cooperated with his office during the entire process of the investigation. The controller furnished most of the documentation requested in a timely manner, and accepted to schedule meetings at a short notice.

XV.VII.VI. Article 83(2)(g) of the Regulation

211. In the assessment of the categories of personal data affected by the infringement, the Commissioner gave due regard to the fact that the combination of personal data is typically more sensitive than a single piece of personal data[100], and that special categories of personal data require enhanced protection due to their sensitivity[101].

212. In the present case, the controller processed several categories of personal data without a valid lawful basis, including biographical details, electoral details, contact details and information revealing the political opinions of the affected data subjects. The combination of these data fields and the involvement of a special category of personal data reveal a high level of intrusiveness to a person's private life.

XV.VII.VII. Article 83(2)(h) of the Regulation

213. The manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller notified the infringement, is another important factor in the assessment carried out under article 83(2) of the Regulation.

[99] Supra, sections XI.II. and XI.III.

[100] WP250, page 24.

[101] Supra, para. 128.

214. As outlined above[102], the Commissioner was initially informed about the incident by the Foundation, and not by the controller. In a manner that the Commissioner considers to be negligent, the controller complied with its obligation to notify his office about the incident almost one (1) month later. This was only after such incident was made public by the media, thus disregarding its statutory reporting duty imposed by article 33 of the Regulation. In this regard, the Article 29 Working Party provides that *"a data controller/processor who acted carelessly without notifying, or at least not notifying all the details of the infringement due to a failure to adequately assess the extent of the infringement* ***may also be considered by the supervisory authority to merit a more serious penalty i.e. it is unlikely to be classified as a minor infringement****"* [emphasis has been added].

XV.VII.VIII. Article 83(2)(k) of the Regulation

215. Finally, the Commissioner considered that the fact that one hundred and six (106) complaints were filed by individuals who requested the Commissioner to investigate, to the extent appropriate, the subject matter of their complaints following the personal data breach, is an aggravating factor of relevance in the individual case under examination.

XV.VIII. Effectiveness, proportionality and dissuasiveness of the administrative fine

XV.VIII.I. The controller as an undertaking

216. Article 83(1) of the Regulation stipulates that each supervisory authority shall ensure that the imposition of administrative fines in respect of infringements of the Regulation shall in each individual case be effective, proportionate and dissuasive.

217. The requirements of effectiveness, proportionality and dissuasiveness of the administrative fine translate into the suitability of the corrective measure to adequately respond to the nature, gravity and consequences of the infringements, and to bring the processing operation into compliance with the rules and, or to punish unlawful behaviour. Such assessment should be carried out by the supervisory authority on a case-by-case basis, and to the extent appropriate[103].

[102] Supra, para. 4.

[103] WP253, page 6.

218. Meeting the tripartite obligation to impose an administrative fine which is effective, proportionate and dissuasive, in the specific case, requires the supervisory authority to use the notion of undertaking[104].

219. Recital 150 of the Regulation refers to articles 101 and 102 of the Treaty on the Functioning of the European Union[105] ("**TFEU**"), which mentions the notion of "undertaking" in connection with administrative fines under the Regulation.

220. The TFEU does not provide a definition of "undertaking", however the CJEU interpreted this term in its settled case-law in a more functional manner rather than in an institutional one[106]. In this regard, the Court ruled that "*[t]he concept of an undertaking encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed*"[107]. The CJEU defined an economic activity as "*[a]ny activity consisting in offering goods and services on a given market*"[108].

221. During the investigation, it was established that the controller's main area of business activity is the delivery of IT services to local clients. The auditor has also reported that "*C-Planet is a small organisation offering software development and managed IT services to local clients*". On the basis of these facts, the Commissioner concluded that the controller is indeed an undertaking.

XV.VIII.II. Effectiveness

222. The requirements of effectiveness, proportionality and dissuasiveness of the corrective measures are recurrent in both the codified Union law[109] and the case-law of the CJEU[110].

[104] Ibid.

[105] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (2012/C 326/01) published on the Official Journal C 326-1 of the 26th October 2012.

[106] Inter alia, *Opinion of Advocate General Jacobs of 22 May 2003*, C-246/01, ECLI:EU:C:2003:304, para. 25.

[107] Judgement of the Court (Sixth Chamber) of 23 April 1991, *Klaus Höfner and Fritz Elser and Macrotron GmbH*, C-41/90, ECLI:EU:C:1991:161, para. 21.

[108] Judgement of the Court (Fifth Chamber) of 25 October 2001, *Ambulanz Glöckner and Landkreis Südwestpfalz*, C-475/99, ECLI:EU:C:2001:577, para. 19.

[109] Inter alia, article 23 of Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC.

[110] Inter alia, Judgment of the Court of 21 September 1989, *Commission of the European Communities v. Hellenic Republic*, C-68/88, ECLI:EU:C:1989:339, para. 24.

223. The requirement of effectiveness is relative rather than absolute, and this translates into the calibration of the amount of the penalty based on the circumstances of the case. These include, on the one part, the specific character of the infringements and, on the other part, the subjective characteristics of the controller, or of the processor, responsible for the infringements[111]. This two-fold assessment is aimed at ensuring that the sanction is suitable to achieve the desired goal, which is the observance of the rules[112].

224. In order to ensure that the requirements of effectiveness, proportionality and dissuasiveness of the administrative fine in the individual case are reconciled with the specificity of the infringements concerned, the Commissioner gave due account to the criteria identified pursuant to article 83(2) of the Regulation[113].

225. As of the subjective features of the controller, at the outset, the Commissioner framed his considerations around, and has taken into account, the specific needs of micro, small and medium-sized enterprises in the application of the Regulation[114].

226. Pursuant to article 2(3) of the Annex to Commission Recommendation 2003/361/EC, "*[w]ithin the SME category, a microenterprise is defined as an enterprise*[115] *which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million*".

227. The Commissioner obtained from the controller the amount of its annual turnover for the years 2018, 2019 and 2020, and confirmed that this amount did not exceed EUR 2 million in any of

[111] European Data Protection Board, *Binding Decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR* ("**EDPB 1/2021**"), para. 414.

[112] "*Effectiveness requires that the sanction is suitable to achieve the desired goal, i.e. observance of the rules*" in European Commission, *Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law* (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2011) 573 final 3, 20 September 2011 ("**COM 573**"), page 9.

[113] Supra, section XV.VII. See also EDPB 1/2021, para. 416.

[114] "*In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation*" in recital 13 of the Regulation.

[115] Article 1 of the same Annex provides that "*[a]n enterprise is considered to be any entity engaged in an economic activity, irrespective of its legal form. This includes, in particular, self-employed persons and family businesses engaged in craft or other activities, and partnerships or associations regularly engaged in an economic activity*".

these years. Having additionally confirmed that the controller had three (3) employees at the time of the incident[116], and therefore, the Commissioner concluded that the controller is a micro-enterprise within the SME category.

228. As a second step in the determination of the effectiveness of the administrative fine, the Commissioner assessed the financial position of the controller[117], by referring to objective criteria in order to define the size of the undertaking measured in terms of its annual turnover[118]. In this regard, the Commissioner noted the EDPB's stance[119] that the turnover[120] of an undertaking is not exclusively relevant to calculate the maximum amount of the fine in accordance with article 83(4)-(6) of the Regulation. Therefore, the Commissioner took into account the controller's turnover as one determining factor to ensure that the fine is effective, proportionate and dissuasive pursuant to article 83 of the Regulation.

229. Considering the requirements deriving from the provisions of the Companies Act (Cap. 386), which place an obligation on directors of public and private companies incorporated in Malta to file certain statutory forms, *inter alia*, their annual accounts, which are then made public by the Registrar of Companies. For this purpose, the Commissioner examined publicly available records to seek information about the controller's annual turnover for the years 2018, 2019 and 2020.

230. The result of these searches proved in the negative and consequently, the Commissioner proceeded to request such financial statements directly from the controller. In its reply, the Commissioner was informed that the accounts for the requested years were not readily available and were being prepared at the time of the request. The Commissioner therefore instructed the controller to submit a declaration signed by a person holding a warrant issued in terms of article 3(2) of the Accountancy Profession Act (Cap. 281), confirming its annual turnover for these years. The information has been duly provided to the Commissioner and it was established that the annual turnover generated by the controller for the years 2018, 2019 and 2020 was EUR 99,789.00, EUR 116,855.00 and EUR 112,533.00 respectively.

[116] Supra, para. 67.

[117] EDPB 1/2021, para. 414.

[118] "*The connection is made between the size of the undertaking, measured in terms of turnover, and the magnitude a fine needs to have in order to be effective, proportionate and dissuasive. In other words, the size of an undertaking - measured in terms of turnover – matters*" in EDPB 1/2021, para. 408.

[119] Ibid., para. 412.

[120] In this decision, "turnover" shall mean the amounts derived from the sale of products and the provision of services after deducting sales rebates and value added tax and other taxes directly linked to turnover.

XV.VIII.III. Proportionality

231. In line with the proportionality requirement, the sanction should be commensurate with the gravity of the conduct and its effects and must not exceed what is necessary to achieve the aim[121]. This implies that the severity of the penalty should be proportionate to the seriousness of the infringements for which it is imposed, which infringements should be viewed as a whole, including their gravity[122].

232. The ultimate aim to be achieved, as contemplated in the Regulation, is to ensure a consistent and high level of protection for natural persons, and a consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons. In order to attain such purpose, supervisory authorities are granted "*equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States*"[123].

233. The Commissioner extensively examined the controller's conducts which resulted in the infringement of multiple provisions of the Regulation, with a particular focus on the gravity of the infringements[124]. Furthermore, due regard was given to the prejudicial consequences of such conduct, and the actions taken by the controller to limit the ramifications arising therefrom.

XV.VIII.IV. Dissuasiveness

234. The requirement of dissuasiveness entails that sanctions constitute an adequate deterrent[125]. According to the CJEU, the severity of penalties must be commensurate with the seriousness of the infringements for which they are imposed, in particular, by ensuring a genuinely dissuasive effect, while respecting the general principle of proportionality[126].

[121] COM 573, page 9.
[122] EDPB 7/2021, para. 415.
[123] Recital 11 of the Regulation.
[124] Supra, section XV.VII.I.
[125] COM 573, page 9. See also EDPB 1/2021, para. 415.
[126] Judgment of the Court (Fourth Chamber) of 27 March 2014, *LCL Le Crédit Lyonnais SA v Fesih Kalhan*, C-566/12, para. 45.

235. Dissuasiveness is therefore related to, and limited by, proportionality. The deterrent effect of the administrative fine cannot exceed what is commensurate with the gravity of the conduct and its effects, and must not exceed what is necessary to achieve the aim of the violated provisions.

On the basis of the foregoing considerations, the Commissioner hereby decides:

i. **that the controller infringed the following provisions of the Regulation in relation to the activity involving the processing of personal data contained in the database file stored on the compromised server:**

   a. **articles 6(1), 9(1) and 9(2);**

   b. **article 14;**

   c. **article 5(1)(f); and**

ii. **that the controller infringed articles 33(1) and 34(1) of the Regulation for not having notified the incident to the Commissioner and the data subjects.**

On the basis of the foregoing legal and technical analysis, and after having taken into account, in particular, the gravity and nature of the infringements, the fact that the controller is a microenterprise, its annual turnover for the years 2018, 2019 and 2020, in terms of article 58(2)(i) of the Regulation, the Commissioner is hereby imposing an administrative fine on the controller of sixty-five thousand Euro (EUR 65,000.00).

Such administrative fine shall be paid within twenty (20) days from the date of receipt of this legally-binding decision.

By virtue of article 58(2)(d) of the Regulation, the Commissioner is hereby ordering the controller to erase with immediate effect the personal data contained in the database file stored on the compromised server and provide the Commissioner with evidence thereof, provided that such order does not prejudice any on-going judicial proceedings.

The controller is hereby being informed that pursuant of article 26(1) of the Data Protection Act (Cap. 586 of the Laws of Malta), any person to whom a legally binding decision of the Commissioner is addressed, shall have the right to appeal in writing to the Information and Data Protection Appeals Tribunal within twenty days from the service of the said decision as provided in article 23 thereof.

Ian Deguara
Information and Data Protection Commissioner