COMPLAINT TO THE DATA PROTECTION AUTHORITY OF MALTA

***noyb* case C-031**

Filed by

[redacted] born on [redacted] and residing in [redacted]

[redacted], born on [redacted] and residing in [redacted]

[redacted] and residing in [redacted],

hereinafter "the Complainants", all citizens of Malta and registrants of the Maltese General Election Electoral Register.

represented by

***noyb* - European Centre for Digital Rights**, a non-profit organisation (see Attachment 1) with its registered office at Goldschlagstraße 172/4/2, 1140 Wien, AUSTRIA, and with registration number ZVR: 1354838270 (hereinafter "*noyb*") pursuant to Article 80.1 GDPR (see Representation Agreement in Attachments 2a, 2b, and 2c)

against

C-Planet (IT Solutions) Limited, Telemetry House, 52, Conservatory Street, Floriana, Malta, an IT services company offering technological support to local and international businesses, with company number C 41536 (hereinafter "C-Planet")

and

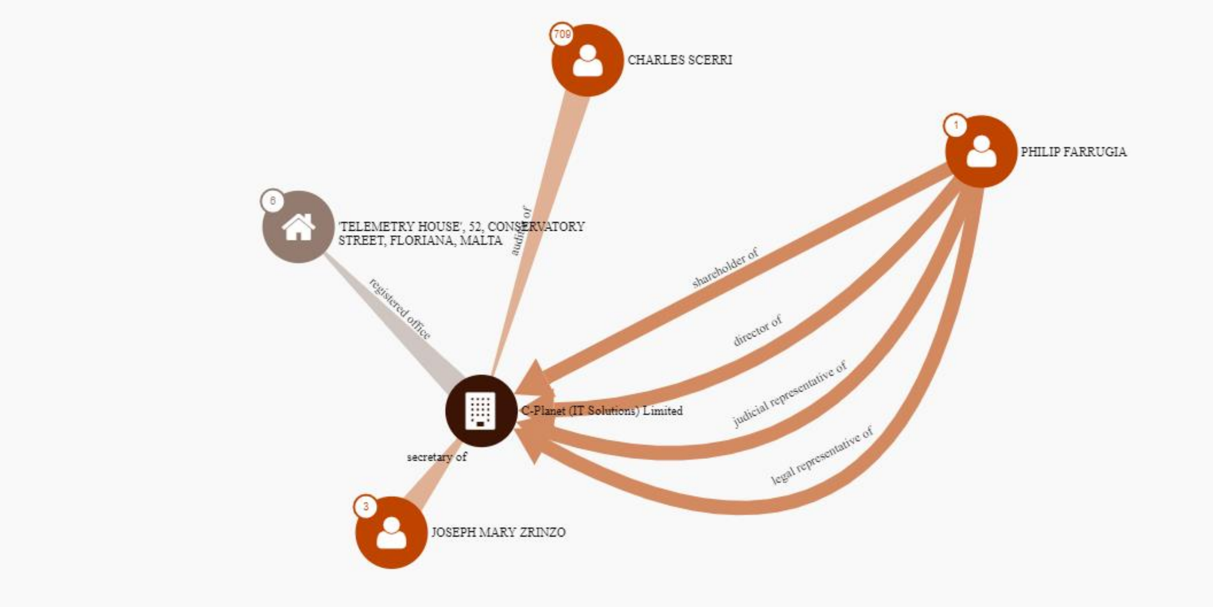
any other controller or processor which the competent data protection authority would identify in the context of this complaint.

1 Facts of the Complaint

1.1 C-Planet

C-Planet was incorporated on 1 June 2007. At the time of the filing, C-Planet's website, [http://www.cplanetmalta.com], was inactive, though it had an active Facebook Page. According to a report by Malta Today (Attachment 3), C-Planet provides IT services for the local councils of Valletta, Bormla, Mdina, Isla, Birgu, St Paul's Bay, Ta' Xbiex, Marsaxlokk, Marsaskala, Birzebbugia, Floriana, Sliema, Santa Venera, Naxxar, and Qormi.

The details of the structure of C-Planet are unclear and may require further investigation by the IDPC. According to the Malta Business Registry, Philip Farrugia is the director, shareholder, legal representative and judicial representative of C-Planet. The figure below, from Paradise Papers Database, shows the structure of C-Planet and the role Philip Farrugia.



According to reporting by the Times of Malta, Philip Farrugia is also a former production director at One Productions. One Productions is the media wing of the Partit Laburista (hereinafter the "Labour Party"), also shareholder in One Productions Limited.

Finally, Mr Farrugia is the brother-in-law of Stefan Zrinzo Azzopardi. Mr Zrinzo Azzopardi has been the Maltese Labour Party's Parliamentary Secretary for European Funds since January 2020. In light of the facts established above, C-Planet appears to be connected to the Labour Party, which publicly distanced itself from the data breach at the core of this complaint.

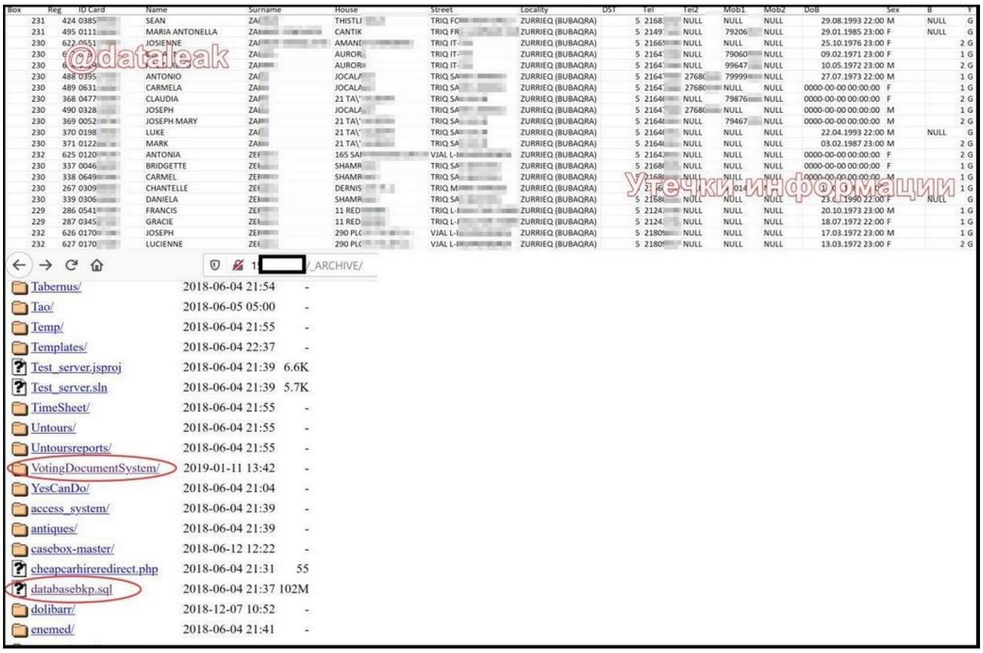
The question of whether C-Planet acted on behalf of another person or organisation (political or not) and processed the data as a controller or processor is still unclear and may require further investigation by the IDPC.

1.2 The data breach at stake

According to reporting by the Times of Malta (Attachment 4), the database at the heart of this complaint is named "**Elec_Registry**" (hereinafter "the Database"), and is contained within a 102MB file hosted by C-Planet (Attachments 5 and 6).

The Database is managed using MySQL, a database administration software that is open source. The use of such software means that information contained within a database can be accessed using a simple web browser since the information on the web server was unencrypted.

Regarding the personal data within the Database, there are multiple basic identifiers for each data subject, including a ballot box number, an ID card number, name, surname, address, telephone number, date of birth, sex and political opinion (the final "Y" column below).



Box	Reg	ID Card	Name	Surname	House	Street	Locality	DST	Tel	Tel2	Mob1	Mob2	DoB	Sex	B	Y
231	424	0385	SEAN	ZA	THISTL	TRIQ FO	ZURRIEQ (BUBAQRA)	5	2168	NULL	NULL	NULL	29.08.1993 22:00	M	NULL	G
231	495	0111	MARIA ANTONELLA	ZA	CANTIK	TRIQ FR	ZURRIEQ (BUBAQRA)	5	2149	NULL	79206	NULL	29.01.1985 23:00	F	NULL	G
230	622	0551	JOSIENNE	ZA	AMANI	TRIQ IT-	ZURRIEQ (BUBAQRA)	5	2166	NULL	NULL	NULL	25.10.1976 23:00	F	2	G
230	6[illegible]	[illegible]	[illegible]	ZA	AUROR	TRIQ IT-	ZURRIEQ (BUBAQRA)	5	2164	NULL	79060	NULL	09.02.1971 23:00	F	1	G
230	6[illegible]	[illegible]	[illegible]	ZA	AUROR	TRIQ IT-	ZURRIEQ (BUBAQRA)	5	2164	NULL	99647	NULL	10.05.1972 23:00	M	2	G
230	488	0395	ANTONIO	ZA	JOCALA	TRIQ SA	ZURRIEQ (BUBAQRA)	5	2164	2768	79999	NULL	27.07.1973 22:00	M	1	G
230	489	0631	CARMELA	ZA	JOCALA	TRIQ SA	ZURRIEQ (BUBAQRA)	5	2164	2768	NULL	NULL	0000-00-00 00:00:00	F	1	G
230	368	0477	CLAUDIA	ZA	21 TA\'	TRIQ SA	ZURRIEQ (BUBAQRA)	5	2164	NULL	79876	NULL	0000-00-00 00:00:00	F	2	G
230	490	0328	JOSEPH	ZA	JOCALA	TRIQ SA	ZURRIEQ (BUBAQRA)	5	2164	2768	NULL	NULL	0000-00-00 00:00:00	M	1	G
230	369	0052	JOSEPH MARY	ZA	21 TA\'	TRIQ SA	ZURRIEQ (BUBAQRA)	5	2164	NULL	79467	NULL	0000-00-00 00:00:00	M	2	G
230	370	0198	LUKE	ZA	21 TA\'	TRIQ SA	ZURRIEQ (BUBAQRA)	5	2164	NULL	NULL	NULL	22.04.1993 22:00	M	NULL	G
230	371	0122	MARK	ZA	21 TA\'	TRIQ SA	ZURRIEQ (BUBAQRA)	5	2164	NULL	NULL	NULL	03.02.1987 23:00	M	2	G
232	625	0120	ANTONIA	ZE	165 SA	VJAL L-I	ZURRIEQ (BUBAQRA)	5	2164	NULL	NULL	NULL	0000-00-00 00:00:00	F	2	G
230	337	0046	BRIDGETTE	ZE	SHAMR	TRIQ SA	ZURRIEQ (BUBAQRA)	5	2168	NULL	NULL	NULL	0000-00-00 00:00:00	F	1	G
230	338	0649	CARMEL	ZE	SHAMR	TRIQ SA	ZURRIEQ (BUBAQRA)	5	2168	NULL	NULL	NULL	0000-00-00 00:00:00	M	1	G
230	267	0309	CHANTELLE	ZE	DERNIS	TRIQ M	ZURRIEQ (BUBAQRA)	[illegible]	2[illegible]	[illegible]	[illegible]014	[illegible]	1[illegible]	[illegible]	1	G
230	339	0306	DANIELA	ZE	SHAMR	TRIQ SA	ZURRIEQ (BUBAQRA)	5	2168	NULL	NULL	NULL	23.[illegible].1990 22:00	F	NULL	G
229	286	0541	FRANCIS	ZE	11 RED	TRIQ L-I	ZURRIEQ (BUBAQRA)	5	2124	NULL	NULL	NULL	20.10.1973 23:00	M	1	G
229	287	0345	GRACIE	ZE	11 RED	TRIQ L-I	ZURRIEQ (BUBAQRA)	5	2124	NULL	NULL	NULL	18.07.1972 22:00	F	1	G
232	626	0170	JOSEPH	ZE	290 PL	VJAL L-I	ZURRIEQ (BUBAQRA)	5	2180	NULL	NULL	NULL	17.03.1972 23:00	M	1	G
232	627	0170	LUCIENNE	ZE	290 PL	VJAL L-I	ZURRIEQ (BUBAQRA)	5	2180	NULL	NULL	NULL	13.03.1972 23:00	F	2	G

1[redacted]/_ARCHIVE/

```
Tabernus/                 2018-06-04 21:54    -
Tao/                      2018-06-05 05:00    -
Temp/                     2018-06-04 21:55    -
Templates/                2018-06-04 22:37    -
Test_server.jsproj        2018-06-04 21:39 6.6K
Test_server.sln           2018-06-04 21:39 5.7K
TimeSheet/                2018-06-04 21:55    -
Untours/                  2018-06-04 21:55    -
Untoursreports/           2018-06-04 21:55    -
VotingDocumentSystem/     2019-01-11 13:42    -
YesCanDo/                 2018-06-04 21:04    -
access_system/            2018-06-04 21:39    -
antiques/                 2018-06-04 21:39    -
casebox-master/           2018-06-12 12:22    -
cheapcarhireredirect.php  2018-06-04 21:31   55
databasebkp.sql           2018-06-04 21:37 102M
dolibarr/                 2018-12-07 10:52    -
enemed/                   2018-06-04 21:41    -
```

Source: Under the Breach, 31 March.

Access to the Database was discovered by security researcher Alex Gor [Twitter username: "@0xyzq"] who published details of the vulnerability of C-Planet's server on Twitter on 29 February 2020 (Attachment 7). Online monitoring service Under the Breach republished Gor's findings on 31 March 2020, stating that the file was "exposed without any security" (Attachment 8).

By using the SQL software to manage the Database, the significant volume of unanonymised personal data contained within the Database, was accessible to anybody on the Internet without any security checks or passwords. It is not clear for how long the Database existed in this form, nor who had accessed it before its discovery was reported.

The Daphne Foundation hosted until November 2020 a free search tool (Attachment 9) which demonstrated the simplicity of identifying a particular individual within the Database, and the extent of the information that the Database contains on them. While this tool did not reveal the specific data pertaining to these categories, it still showed the quantity of personal data that C-Planet collected and kept about the data subjects.

1.3 Content of the Database

The Database contains several categories of information relating to the data subject as an identifiable natural person. This complaint organises these categories into three groups.

1.3.1 Publicly available personal data

The first group comprises the data subjects' names and surnames, ID card numbers, and addresses. This information is available to the general public at any time without security checks or passwords, via the Electoral Commission of Malta's General Election Electoral Register (hereinafter the "Electoral Register", see attachment 10).

Under Article 30(3) of the Malta General Elections Act (hereinafter "the General Elections Act"), *"The Electoral Register shall be compiled in such manner that the public may be aware of the persons who are registered as voters*", clarifying that the purpose of processing this data is limited to public awareness.

1.3.2 Not publicly available personal data

The second group concerns the data subjects' ballot box number, voting document number, telephone number and gender. This information does not appear on the Electoral Register.

1.3.2.1 Data ballot box and voting document number

According to Article 64.1.b of the General Elections Act, the Electoral Commission shall forward copies of the lists of eligible voters to all political parties contesting the general election prior to the day of voting. The lists must identify:

- the polling booth where each voter exercises their right to vote;
- a "distinct and consecutive" voting number;
- the registered number of each individual voter's voting document.

Article 64.1.b also makes clear that only political parties are entitled to have access to this information. The exemplar voting document in the Seventh Schedule of the General Elections Act confirms that these lists include data pertaining to an individual data subject's ballot box and voting number (Attachment 11).

1.3.2.2 Data subject gender and telephone number

This information neither appears in the Electoral Register nor in the General Election Act requirements. Therefore, to compile the Database, these categories of data must have been collected by the creator of the Database and combined with the data on the Electoral Register and the data provided to the political parties by the Electoral Commission.

1.3.3 Political opinions

The third group concerns the data subjects' political leaning. According to the Times of Malta (Attachment 12), the Database comprises a numerical identifier from 1 to 4, denoting a data subject's political preference. The number '1' would classify the data subject as a Labour Party supporter, and '2' as a suspected Nationalist Party supporter. The meaning of numbers '3' and '4' is still unknown.

Similar to the data described in 3.2.1 and 3.2.2., this data is not available via the Electoral Register under the General Elections Act. It must have been added to the Database by C-Planet. The source of the data concerning the political opinion of the voters is unknown to us.

1.4 Size of the Database

According to the original report by Under the Breach, the Database contains the personal data of 337,384 Maltese citizens eligible to vote in Malta (hereinafter "voters").

According to the most recent figures available from the Electoral Commission of Malta from 2017, there are 341,856 voters on the Electoral Register.

According to Eurostat, the most recent figure for the population of Malta as a whole, from 2019, is 493,559 people. Therefore:

- The Database contained the personal data of about 68% of the Maltese population.
- The Database contained the personal data of about 98% of the Maltese electorate.

1.5 Period when the Database was accessible

As noted in section 2 above, personal data contained in the Database were made available to anyone, with no password or other form of security or authentication required to access it.

Regarding the timeframe of accessibility, Alex Gor published details of the vulnerability of C-Planet's server on Twitter on 29 February 2020. According to a report by Malta Today, *"the hole in the server was only closed around 9th March [2020]."*

The dates above suggest that there was a window of at least ten days where the sensitive personal data of 98% of Maltese voters was publicly known and available online to anyone.

1.6 Reaction by C-Planet

According to the report by Malta Today, C-Planet was notified via email of the vulnerability of the Database *"in February, but there was no reaction".*

In a report by the Times of Malta 1 April 2020, the Maltese Information and Data Protection Commission (hereinafter the "IDPC") Deputy Commissioner Ian Deguara states:

> *"We got to know about this personal data breach this morning from media reports. We shall trigger our investigation procedure with the controller responsible for the processing to establish all the facts surrounding this security incident."*

According to the same report, representatives for C-Planet claimed that it had *"immediately"* alerted authorities *"upon the notification of the alleged breach"*. C-Planet offered as a justification that the breach was a "mishap" comprising "old" data.

It appears from the above that there are several factual discrepancies concerning the timeline of the breach suggesting that C-Planet did not notify the IDPC.

2 Grounds for the Complaint

This complaint is filed against C-Planet, without determining whether C-Planet acted as the controller of the database or processed the data on behalf of another entity. However, considering the nature of the data, it is requested that the IDPC investigates whether C-Planet acted as processor for an organisation involved in politics. Should the IDPC conclude that another entity acted as the controller in this case, this complaint shall be read to apply to that entity accordingly.

The grounds for the complaint consist of three issues. Each of them consists of multiple violations, each pertaining to a specific GDPR provision. The three issues are:

1) the illegal collection and processing of the data by C-Planet,

2) the failure to inform data subjects and the “secret” collection of data on the population, and

3) the violation of data security laws and principles by C-Planet.

2.1 The illegal collection and processing of the data by C-Planet

The lack of any lawful basis for the processing of the data at stake and the violation of the purpose and storage limitations principles form the subject matter of the first issue in this complaint.

2.1.1 No legal basis for processing (violation of Article 6 GDPR)

Article 6.1 GDPR makes clear that a processing can only take place on the basis of one of the six exhaustive legal bases mentioned in this provision. None of these six bases apply to C-Planet’s processing of the personal data of Maltese voters.

The Maltese citizens –including the Complainants- did not give their consent to the processing of the data at the core of this complaint. Nor were they bound by a contract with C-Planet or any other entity in relation to the Database. We are not aware of any legal obligation that necessitate C-Planet collecting and keeping personal data of 98% of the electorate of any entire state, which also makes Article 6.1.c GDPR not applicable. Furthermore, the processing is not necessary for the protection of the vital interests of the individuals, and C-Planet is not vested in any mission of public interest.

Finally, Article 6.1.f provides a lawful basis for processing necessary for a legitimate interest of the controller or a third party, and does not override the interests or fundamental rights and freedoms of the data subjects. Even if C-Planet could identify such a legitimate interest, it is clear that the processing at stake would not pass the balancing test, on the basis of various elements mentioned in the Opinion 6/2014:

- individuals cannot “reasonably expect” that their information will be aggregated into a mass database with their other personal details and political opinions by an IT company with which they never had contact before;
- the potential harmful impact of the processing on the population is quite obvious (risk of discrimination, exclusion, and damage of individuals’ autonomy);
- the nature of some of the data is very sensitive (political opinions);
- this large scale processing was made available to a vast number of persons during several days;
- no security measures were implemented to prevent accidental disclosure.

Considering the above, the processing cannot not rely on any of the 6 exhaustive legal bases of Article 6.1 GDPR. This processing is therefore unlawful.

2.1.2 Illegal processing of sensitive data (violation of Article 9 GDPR)

Under Article 9.1 GDPR, the "*processing of personal data revealing [...] political opinions, [...] shall be prohibited.*" The "political leaning" information contained in the Database clearly falls under Article 9.1. Therefore, in addition to a legal basis under Article 6.1 the controller needs a basis under Article 9.2 GDPR:

Given the inapplicability of any the exceptions to this prohibition under Article 9.2 GDPR, it is clear that C-Planet was involved in the illegal processing of sensitive data.

2.1.3 *In the alternative:* Violation of Article 9 GDPR of a privileged controller

Only in the case that the investigation reveals that C-Planet was acting on behalf of a controller involved in political activities, the sections 2.1.3.1 and 2.1.3.2 below conclude to the inapplicability of Article 9.2.d and 9.2.g exceptions to the processing at stake.

2.1.3.1 Processing not carried out by in course of legitimate activities (Article 9.2.d GDPR)

Article 9.2.d GDPR permits the processing of sensitive data where the processing is carried out by a foundation or other not-for-profit body with a political aim provided the processing is in the course of its legitimate activities and is subject to appropriate safeguards.

While C-Planet is not considered a foundation or not-for-profit body for the purposes of Article 9.2.d, there may be other controllers identified in the course of an investigation to whom such a classification would apply. Even so, the manner in which Maltese voters' political personal data revealing was processed still constitutes a violation of Article 9.2.d regardless of the identity of the controller.

First, for data to be processed lawfully under Article 9.2.d, the processing must be carried out with "appropriate safeguards". Given C-Planet's actions (or lack thereof) resulted the widespread and unauthorised access to the Maltese voters' sensitive data, and the violation of multiple core processing principles, it is clear these were not provided.

Second, for the Article 9.2.d exception to apply, the processing must also only be carried out on data revealing the political opinions of members or former members of the body, or persons having regular contact with the body. The former does not apply as processing the personal data of 98% of Maltese voters will inevitably involve data subjects with no affiliation. The latter does not apply due to the scale of the processing at stake; it is hard to understand how data subjects who are not members of a political party could be considered to have "regular contact" with them.

Finally, Article 9.2.d cannot apply if the personal data in question was disclosed outside the body without the data subjects' consent. This is clearly the case as the Database was accessible to anyone outside of C-Planet.

2.1.3.2 Processing of data revealing political opinions not in substantial public interest (Article 9.2.g and Recital 56 GDPR)

Should the IDPC discover that the processing of sensitive data was conducted on behalf of a political organisation, this complaint clearly establishes that the exceptions under 9.2.g GDPR do not apply for the reasons set out below.

Recital 56 provides:

> *"Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established"*.

There is no law in Malta allowing the compilation or long-term storage of political voter data

As outlined above, no part of the General Election Act suggests that political parties are entitled to keep voter information like the personal data in question here after the conclusion of an election, and in no event is the processing of political opinions allowed under the law. Keeping data in a form which permits identification of the data subjects for longer than is necessary violates Article 5.1.e GDPR.

There are no appropriate safeguards established

Given the widespread and unauthorised access to the Maltese voters' sensitive data, and the violation of multiple core processing principles, it is clear that no appropriate safeguards were provided.

2.1.4 Violation of the storage limitation principle (Article 5.1.e GDPR)

It is clear that the processing activities at the heart of this complaint violate the principle of storage limitation (Article 5.1.e GDPR), particularly where the personal data was kept in a form permitting the identification of the data subjects "for longer than is necessary".

The following demonstrate the respondents' outright violation of this principle:

- Malta has clear electoral rules regarding time limits for accessing and using data from its Electoral Register. However, some of the information in the Database was approximately seven years old and predated the 2013 elections;
- All the data subjects in the Database were identifiable at the time of the data breach. There was no anonymisation or even pseudonymisation of any elements of the data subjects' identities. In fact, the identity of every data subject was so specific that any person accessing the Database had no trouble tracing a particular individual to their home, private telephone line or political leaning;
- In a flagrant disregard for obeying the law and safeguarding data subject rights, C-Planet even admitted in their initial press statement to the Times of Malta that the data was "old".

2.1.5 Violation of the purpose limitation principle (Article 5.1.b GDPR)

Article 5.1.b requires personal data to be collected for "specified explicit and legitimate purposes", and not processed further in a manner incompatible with these initial purposes.

The Database was compiled from several sources, most notably via the aggregation of public electoral data with additional fields entered by third parties. It seems that the data processed under 1.3.1. and 1.3.2. were originally collected and used in the context of an electoral campaign. However, they were clearly used in violation of the original purpose. One should indeed remember that the General Elections Act provides that the list of voters is made public for public awareness, not to allow organisations to build database with the political opinions of these voters. The processing of data by C-Planet therefore violates Article 5.1.b GDPR.

2.2 The secret collection and processing of political data on the population (violation of Articles 12, 13 and 14 GDPR)

At the core of this case is the secret collection, by a private entity, of the political opinions of nearly every single individual entitled to vote in Malta. In carrying out such activities, C-Planet has not only violated several provisions of the GDPR; it has also directly placed data subjects in a situation where their rights and freedoms are rendered precarious, vulnerable and violated without their knowledge.

Article 12 GDPR sets out the preliminary requirements for controllers to act with transparency in order to facilitate data subjects' enforcement of their data protection rights. The Complainants never received the information under Article 12.1, namely the information relevant for Articles 13 and 14, Articles 15-22, and Article 34 GDPR.

The Transparency Guidelines, paragraph 27, stipulate that where either Article 13 or Article 14 apply, *"providing [personal data] in a timely manner is a vital element of the transparency obligation and the obligation to process data fairly".*

In fact, without the data breach and if the Daphne Foundation tool had not become available at all, it is likely that the Complainants would never have discovered this secret Database and the multitude of violations of their rights.

2.3 Violation of data security laws and principles

The breaches below, in particular the data breach and subsequent failure to notify by C-Planet, illustrate the extent to which C-Planet violated the integrity and the confidentiality of the data of the people of Malta, and their subsequent failure to remedy such a violation.

2.3.1 Violation of data integrity and confidentiality (Article 5.1.f GDPR)

Article 5.1.f requires personal data to be processed in a manner that ensures its security, "*including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*". For the reasons listed below, it is clear that the controller failed to process the personal data in such a manner:

- C-Planet's choice of security measures (or lack thereof) permitted the data to be available to the wider public without any authorisation requirements;
- the subsequent availability of the data left it vulnerable to further unauthorised or unlawful processing that should never have had occurred in the first place;

- C-Planet's apparent failure to use appropriate technical and measures culminated in a breach of Articles 32.1 and 32.2 GDPR.

2.3.2 Failure to implement appropriate security measures (Article 32 GDPR)

Article 32.1 GDPR requires the controller and processor to implement "*appropriate technical and organisational measures to ensure a level of security appropriate to the risk*". To determine whether such measures could be considered "appropriate", several factors must be accounted for, including the state of the art, the costs of implementation, the nature, scope, context and purposes of processing, and the risk of varying likelihood and severity for the rights and freedoms of natural persons. C-Planet clearly failed to reach this mark, and thus violated Article 32 GDPR.

2.3.2.1 Violation of Article 32.1 GDPR

C-Planet failed to implement appropriate technical and organisational measures given its failure to properly account for the following factors:

- **State of the Art**

The A29WP Guidelines on data breach notification (hereinafter "the Data Breach Guidelines") accept that the technology considered to be "state of the art" for technical and security purposes can change over time, but the onus is on the controller to ensure their security arrangements are up to date. The Data Breach Guidelines use encryption measures as an example of this, where they stipulate that while "*the encryption may* […] *be considered currently adequate by security experts, it may become outdated in a few years' time, meaning it is questionable whether the data would be sufficiently encrypted by that product and provide an appropriate level of protection*." The European Union Agency for Cybersecurity (ENISA) Guidelines on "state of the art" in IT security sets out similar expectations.

If this Database has subsisted in some form since 2013, as the facts suggest, it would be expected that the controller has updated their security arrangements on several occasions over the course of seven years. These expectations are all the more justifiable - and prescient - in this particular complaint, given that C-Planet is an IT company with 13 years of operation and expertise in information processing, and a director who claims to have several advanced diplomas in information processing, a multiplicity of certifications from the Maltese National Science Computer Academy, and according to his LinkedIn profile (Attachment 13), over twenty years' experience in the information technology sector.

- **Costs of implementation**

At the time of filing of the complaint, any further information on C-Planet's data processing practices, aside from what is submitted here, was not available. No matter the details of the case, it is submitted that encryption of the data was the minimum requirement for any database and especially when it comes to the Database at stake. Encryption solutions are usually integrated in any database software and adequate open-source encryption is available for free. In other words: it costs nothing to shield personal data from unwanted access.

- **Nature, Scope, Context and Purposes of Processing**

The nature, scope and context of the processing of the data further underscores the degree to which security arrangements employed by C-Planet for this Database were entirely inappropriate:

- the Database included sensitive personal data on the private political leaning of about 98% of the Maltese population eligible to vote. Aside from this Database, this information was not publicly available or searchable in such a format;
- this particular category of data is subject to additional protections under Article 9 GDPR, which immediately suggests that a means of storage used for less sensitive data would not be sufficient in this case, let alone the open source management system C-Planet did use;
- the secret nature of the collection of the data and the lack of information provided to the data subjects by C-Planet suggests that C-Planet was reluctant to reveal the specific purposes of the processing;

These reasons make it difficult to classify the security arrangements implemented by C-Planet as anything beyond careless.

- **Likelihood and severity for the rights and freedoms of natural persons**

The processing of personal data (including political opinions) by a company with connections to a major political party, with no specified context or purpose for processing of the data, and the consequences for the Complainants in case of exposure of their political opinions indisputably establishes a high risk for their rights and freedoms.

2.3.2.2 Violation of Article 32.2 GDPR

Article 32.2 makes clear that when assessing the appropriate level of security, one must take into account the risks presented by the processing, including the unauthorised disclosure of or access to the personal data stored. The Data Breach Guidelines further emphasise that *"the ability to detect, address, and report a breach in a timely manner should be seen as essential elements"* of Article 32.2 considerations.

Following this, the window of accessibility, where the Complainants' personal data was unlawfully made public without their authorisation, demonstrates a blatant failure to appreciate the risks pertaining to the processing. C-Planet's apparent lack of reaction to the breach, only compounds this lack of consideration, which ultimately resulted in a breach of Article 32.2, and Article 32 GDPR more generally.

2.3.3 Violation of Articles 33 and 34 GDPR: no notification to the DPA and to the data subjects

Article 33.1 provides that *"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons".*

Article 34.1 requires the controller to notify data subjects of a personal data breach without undue delay, where the breach "*is likely to result in a high risk to the rights and freedoms of natural persons".*

In order to satisfactorily establish a violation of Articles 33 and 34 GDPR, we outline below:

- that the exposure of the Database on the server was a personal data breach within the meaning of Article 4.12 GDPR (see 2.3.3.1.),

- that the breach in question fulfils the risk criteria as set out in the Data Breach Guidelines and should therefore have been notified to the competent supervisory authority (see 2.3.3.2.) and the data subjects (see 2.3.3.2 and 2.3.3.3).

2.3.3.1 Existence of a personal data breach (Article 4.12 GDPR)

Article 4.12 GDPR 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."

The data in question is personal data within the meaning of Article 4.1, namely that the addresses, ID numbers, full names, voting information and political preferences, all constitute information relating to an identifiable natural person, i.e. the Complainants.

The breach of security in this complaint was the storing of the Database on an open source management system that could be accessed by third parties without further authorisation being required, such as a password or other form of authentication. A29WP Opinion 3/2014 on personal data breach notification classifies this as a confidentiality breach at page 6. According to the Data Breach Guidelines: "*The consequence of such a breach is that the controller will be unable to ensure compliance with the principles relating to the processing of personal data as outlined in Article 5 of the GDPR*" (see page 7).

2.3.3.2 Assessment of the risk

Although the GDPR introduces the obligation to notify a breach, it is not a requirement to do so in all circumstances. Under Article 33, notification to the competent supervisory authority is required unless a breach is unlikely to result in a risk to the rights and freedoms of individuals. Under Article 34, communication of a breach to the individuals is only triggered where it is likely to result in a high risk to their rights and freedoms.

The Data Breach Guidelines include criteria for assessing whether a "risk" for Article 33 or 34 purposes necessitates notification by the controller. If the criteria are fulfilled in either instance, then notification to the relevant supervisory authority, data subjects, or both, is required.

For both Article 33 and 34 in this complaint, the risk criteria are fulfilled. The risks to the affected individuals' rights and freedoms are indisputably high, and C-Planet (or any other controller identified in the context of this complaint) is at fault for failing to notify the IDPC and the data subjects of the breach.

The fulfilment of the criteria is set out below.

- Number of people affected:
  - "*a breach affecting large volumes of personal data about many data subjects can have an effect on a corresponding large number of individuals*";
  - This criterion is fulfilled given that the breach involved the disclosed the personal data of over two-thirds of the population of Malta, and about 98% of the population who were eligible to vote;

- Nature of the data:
  - “*A combination of personal data is typically more sensitive than a single piece of personal data*”;
  - This criterion is fulfilled because the Database at stake included a combination of full names, phone numbers, state and voting ID numbers, addresses, ballot box numbers, and political preferences;

- Ease of identifying individuals:
  - “*An important factor to consider is how easy it will be for a party who has access to compromised personal data to identify specific individuals*”;
  - This criterion is fulfilled given the extent of the data combined in the Database makes it extremely easy to identify a specific individual;
  - Even if some elements of personal data overlapped (e.g. several subjects having the same name or address), the categories providing a unique identifier (e.g. ID and voting document numbers) would allow those individuals to be distinguished almost immediately;

- Severity of consequences:
  - “*the potential damage [in breaches involving special categories of data] to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm*”;
  - This criterion is fulfilled in light of the sensitivity of political opinions and the use that can be done thereof;

- Permanence of consequences:
  - “*Consideration should also be given to the permanence of the consequences for individuals, where the impact may be viewed as greater if the effects are long-term.*”
  - This criterion is likely fulfilled considering that the risk of knowledge of a data subjects’ political preferences may restrict access to employment or financial opportunities for a long term;

- Special characteristics of the controller:
  - “*The nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach*”;
  - Should the investigation establish that a political organisation was the controller of the Database, the risk for individuals would be clearly demonstrated.

In assessing the risks pertaining to Article 34, Recital 85 provides 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 such as […] discrimination […] damage to reputation […] or any other significant economic or social disadvantage to the natural person concerned.*”

Furthermore, under the Data Breach Guidelines:

> *“When the breach involves personal data that reveals […] political opinion […] such damage should be considered likely to occur.”*

> *"It will be obvious [...] due to the nature of the breach and the severity of the risk, the controller will need to notify the affected individuals without delay*".

Given these provisions, it is indisputable that there was a high risk to the data subjects in this case, which in turn should have prompted an expeditious response by C-Planet. Harm is acutely aggravated when data subjects don't know that this information is out there, and that these risks to them now exist.

The data subjects' fears of an increased risk to their rights and freedoms, and an amplified possibility of being subjected to aforementioned damages and disadvantages on release of their political information are not unfounded. The Times of Malta have reported that it would be reasonable *"for a person to fear that they suffered or may suffer discrimination or other consequences because of this very serious leak."* (Attachment 14).

As a conclusion,

- the data breach should have been notified to the IDPC. Besides the risk factors mentioned above, the Data Breach Guidelines stipulate that: *"a failure to comply with Article 33 will exist where a controller does not notify the supervisory authority in a situation where the data has not actually been securely encrypted".*
- the data breach should also have been notified to the data subjects in accordance with Article 34.1 GDPR. In our view, none of the exceptions under Article 34.3 GDPR are applicable as explained below.

2.3.3.3 Non-application of the exceptions of Article 34.3 GDPR

- **No appropriate security measures (Article 34.3.a GDPR)**

Under Article 34.3.a, communication of the breach to data subjects will not be required where the controller implements appropriate technical and organisational protection measures to the personal data affected by the breach.

The developments above clearly establish that no such measures were implemented; while Article 34.3.a states that the use of encryption is a particularly compelling factor for meeting this exemption, it should be noted that the data in this case was not even encrypted.

- **Risks to rights and freedoms likely to materialise (Article 34.3.b GDPR)**

Under Article 34.3.b, communication of the breach to data subjects will not be required where the controller has taken subsequent measures to ensure that the high risks to the rights and freedoms of the data subjects are no longer likely to materialise. The present complaint clearly establishes that such an exemption cannot apply here, considering that the risk to the data subjects still persists today since anyone could access the database for several days, allowing several copies to be done without further control by C-Planet.

- **No disproportionate burden on the controller (Article 34.3.c GDPR)**

Under Article 34.3.c, communication of the breach to data subjects will not be required where such a communication would involve "disproportionate effort" on the part of the controller. In such cases, the controller must instead use a public communication or similar measure to communicate the breach. It is clear that this exemption does not apply, as C-Planet (or the controller) already had the means to directly contact all affected data subjects.

2.3.4 Failure by the processor to meet contractual requirements (Article 28.3)

Article 28.3 provides that the data processing activities of processors must be governed by a binding contract between the processor and controller. This contract must include a number of implied terms pursuant to the GDPR, including:

- 28.3.c – the processor must take all necessary measures to comply with Article 32;
- 28.3.f – the processor must assist the controller in ensuring compliance with Articles 32 to 36 (see also Article 33.2 GDPR);
- 28.3.h – the processor must "immediately" inform the controller if they are of the opinion that one of their instructions from the controller infringes the GDPR.

Should C-Planet be identified as the processor of another entity being the controller of the Database, C-Planet would still be in breach of its obligations under its contractual requirements under Article 28.3 GDPR. In such a case, it should still be determined whether the controller identified by the competent authority met its obligations under Article 28 GDPR.

3 Requests

3.1 Request to investigate

The Complainants hereby requests that you fully investigate this complaint, in accordance with the powers vested in you in particular Articles 58.1.a, 58.1.e and 58.1.f GDPR, to determine:

i. which processing operations have occurred;

ii. the purpose(s) of the processing;

iii. the specific legal basis relied on for each specific processing operation;

iv. any available information as to the source of the data subjects' personal data;

v. the previous, current and future recipients of the personal data;

vi. whether C-Planet was the controller or the processor of the Database;

vii. if relevant, the identity of the controller and whether a proper written contract was in place between controller and processor;

viii. the dates the controller and/or the processor (and any other relevant persons involved) became aware of the breach;

ix. the security measures in place and whether they were sufficient;

Finally, the Complainants would like to request that any results of this investigation are made available to *noyb* in the course of this procedure, in accordance with Article 77.2 GDPR and the right to be heard and/or file additional submissions under the applicable national procedural law.

3.2 Request to compel the controller to erase all personal data and stop the processing

The Complainants also requests that the controllers and/or processors are compelled to erase all unlawfully processed personal data without undue delay and to prohibit the relevant processing operations in accordance with the powers vested in you, including by Article 58.2.d, f, and. g GDPR.

3.3 Request to impose an effective, proportionate and dissuasive fine

Finally, we request that the relevant supervisory authority, by virtue of the powers provided by Article 58.2.i in combination with Article 83.4.a GDPR, impose an effective, proportionate and dissuasive fine against the controllers, taking into account that:

i. the breach in question affects about 98% of the Maltese electorate (Article 83.2.a GDPR);

ii. the controller left highly sensitive data on an open source Database accessible to anyone without a password or other authorisation (Article 83.2.d GDPR);

iii. the controller processed highly sensitive data, including special categories of personal data (Article 83.2.g GDPR);

iv. the controller failed to notify the supervisory authority and the affected data subjects (Article 83.2.h GDPR);

v. the supervisory authority first learnt about the breach from media reports, and not the controller, at least 24 days after the breach occurred (Article 83.2.h GDPR);

vi. the fact that the disclosure of voting preferences renders the data subjects particularly vulnerable to discrimination and social and economic disadvantages (Article 83.2.k GDPR);

vii. a wilful, massive and profound violation by a company processing sensitive political data must be adequately sanctioned to prevent similar violations of the GDPR in the future, and to ensure the protection and safety of individuals that the new data protection acquis seeks to provide.

We request the maximum possible fine under Article 83.4.a GDPR, i.e. 10 million euros or 2% of the worldwide annual turnover of the controller and any processor identified in the course of the investigation, whichever is higher. We believe that the gravity of the case, in particular the multiple breaches and violations by the controller and the scale of the Maltese population affected, necessitates significant sanctions to the controller, both financial and otherwise.

4 Communication

Communications between *noyb* and the Data Protection Authority in the course of this procedure should be done by email at [redacted] with the following reference: *noyb* complaint n°C-031.

Signature