5 September 2022

To:

Adv. Gilad Semama
Privacy Protection Authority Commissioner

Subject: PPA's Preparedness for Protection of Privacy Ahead of 25th Knesset Elections

1. This letter is sent to you by Zulat for Equality and Human Rights, a research institute that acts toward strengthening democracy and protecting human rights, in light of the obligation of the Privacy Protection Authority [PPA] to protect the right to privacy of Israel's citizens in the run-up to the upcoming elections to the 25th Knesset.

2. As will be detailed below, Zulat proposes that the PPA take a series of preemptive steps to safeguard the public's right to privacy in the run-up to the upcoming elections, based on the lessons learned from serious events in the election campaigns of recent years.

3. The right to privacy is explicitly recognized in Article 7 of Basic Law: Human Dignity and Liberty and various other laws, primarily the Protection of Privacy Law,5741-1981 (hereinafter, "Privacy Protection Law),[1] as well as in international treaties (such as Article 17 of the International Covenant on Civil and Political Rights of 1966). The Supreme Court has recognized the right to privacy as one of the freedoms that shape the democratic character of the Israeli regime and guarantee the basic dignity that every human being is entitled to.[2]

4. The PPA is the state entity that regulates, oversees, and enforces the provisions of the Privacy Protection Law. As part of its role, the PPA is entrusted with the protection of personal information in digital databases and with strengthening the right to privacy. The PPA's regulatory role includes administrative and criminal enforcement on all entities in Israel - private, business, and public - that hold or process digital personal information.[3]

5. Elections in the digital age, with online campaigns and private companies providing political parties with voter-prompting platforms, pose serious and everchanging challenges to the protection of the right to privacy and information security. Of particular concern is the abuse of voter privacy, leaks of the Voter Register, and even violation of the integrity of the election process itself.

6. The assumption is that information concerning private individuals, collected and managed by the political parties as part of their election campaigns by either themselves, service providers, or external applications, is a "database" as defined in the Privacy

[1] Protection of Privacy Law, 5741-1981 (Unofficial Translation), *Israel Government's website*.
[2] Supreme Court Ruling HCJ 6732/20, Association of Human Rights in Israel v. Knesset, *Nevo's website*, 1 March 2021 (Hebrew).
[3] Privacy Protection Authority's website, *Justice Ministry's website*, 15 August 2019.

Protection Law and is thus bound by all its requirements, in particular with regard to the level of security and its permitted uses.

7. The recurrent rounds of elections in recent years have proven that adherence to the provisions of the Privacy Protection Law is at the very least shaky, and that in the race for every vote some of the parties are willing to compromise the citizens' right to privacy.

8. As described on the PPA's website,[4] a major incident involved the company Elector Software Ltd., which was given a copy of the Voter Register file to develop the voter-prompting Elector App that the Likud and Yisrael Beytenu used in their election campaign. The first serious security breach occurred on 8 February 2020 when hackers accessed the company's systems and downloaded the file containing data about 6.5 million eligible voters, including personal details, addresses, assigned voting stations, and other sensitive information that had been entered by the parties, such as a voter's medical condition or an indication that they "support" or "do not support" the party.

9. Twenty-four hours after this massive leak, the PPA launched an investigation into the incident in a bid to stop the spill of additional information,[5] yet another serious leak occurred on 16 February 2020.[6] The PPA subsequently determined that the parties had violated the provisions of the Privacy Protection Law and imposed an administrative fine on Elector Software,[7] but the damage had already been done.[8]

10. That a calamity was bound to happen was a foregone conclusion. Only a few days earlier, in an article published on 5 February 2020 in the newspaper Calcalist, journalist Omer Kabir had warned about the danger of just such an incident.[9]

11. In addition, there is the fear about the dissemination of fake news and targeted false/biased information in violation of the provisions about "direct mailing" as interpreted in Directive 2271/2 of the Registrar of Databases,[10] such as failure to specify the sender's identity or the recipient's right to be deleted from a database sending messages.

12. As a lesson learned from the above, in the run-up to the elections to the 24th Knesset, the PPA published detailed guidance about the provisions of the Privacy Protection Law as they apply to the use of the Voter Register/other personal data and about the responsibility borne by the political parties for the use of databases and outsourcing services,[11] and has conducted professional refresher courses for party representatives.[12]

---

[4] Administrative Enforcement Data for 2021, *PPA's website* (Hebrew).
[5] Omer Kabir, Following Likud App Breach, Regulator Descends on Offices of Suspected Developer, *calcalisttech.com*, 11 February 2020.
[6] Omer Kabir, Nothing Fixed: Voter Registry Again Hacked From Elector, *calcalist.co.il*, 16 February 2020 (Hebrew).
[7] Data on Administrative Enforcement in 2021, *PPA's website* (Hebrew).
[8] Omer Kabir, Following Likud App Breach, Regulator Descends on Offices of Suspected Developer, *calcalisttech.com*, 11 February 2020.
[9] Omer Kabir, Nothing Fixed: Voter Registry Again Hacked From Elector, *calcalist.co.il*, 16 February 2020 (Hebrew).
[10] Directive 2271/2 of Registrar of Databases, *Law, Information, and Technology Authority's website*, 21 June 2017 (Hebrew).
[11] Privacy Protection Law Requirements in Run-Up to 24th Knesset Elections, *PPA's website*, 7 January 2021 (Hebrew).
[12] Attorney Ely Calderon, Highlights of Proper Conduct Regarding Use of Databases, presentation at PPA

13. Ahead of the upcoming elections, the PPA published similar guidance, but this time it included the appendices "Highlights and Recommendations Based on Previous Election Campaigns,"[13] "Guidelines to Companies Providing Technological Services to Political Parties,"[14] and "Guidelines for Training Employees/Volunteers During Election Campaign."[15]

14. These are welcome initiatives attesting to a positive process of lessons learned but they are not enough, given that in the digital age it is impossible to "recall" information that is already online. Nor is the toolbox at the PPA's disposal deterrent or persuasive enough to compel political parties to devote thought and resources to the matter at a time when they are busy fighting for every voter.

15. Therefore, especially as a lesson learned from the Elector Software case (with the PPA acting only after data about millions of citizens had leaked out, and failing to prevent yet another hacking shortly afterwards), retroactive measures to protect privacy are clearly inadequate and what the PPA needs to do is to take preemptive steps.

16. The PPA must take basic oversight measures, to be detailed below, to verify in advance that its instructions have been internalized and implemented, both by the parties and by their technological service providers.

17. These preemptive measures should apply to information security, the features of the collected data, and the citizens' consent to its collection and use in accordance with Article 2(9) of the Privacy Protection Law and the PPA's guidelines.

18. Although the actions vis-a-vis Elector Software focused on the hacking, the case also highlighted the need for preemptive oversight to ascertain that no use whatsoever is made of data without a person's consent and that the information is not used beyond what was explained to the person from whom it was collected. During the run-up period, it is imperative to obtain the citizens' lawful consent about entering their personal data in party applications/databases and on how it will be used, especially information regarding their support for a party.

19. The importance of preemptive measures was highlighted in Supreme Court Case 1311/20, Adv. Shahar Ben-Meir v. Likud.[16] Rejecting the petition, the court ruled that protecting the privacy of Israel's citizens is not included in the job description of the chairman of the Central Elections Committee, which means that the PPA is the sole body responsible for it during an election period.

20. It should be emphasized that Articles 10(c) and 10(e1) of the Privacy Protection Law are broad enough to allow the PPA to initiate preemptive oversight measures:

course on "Securing Proper Conduct of Parties," *Justice Ministry's website*, 8 February 2021 (Hebrew).

[13] Privacy Protection Law Requirements in Run-up to 25th Knesset Elections, *PPA's website*, 25 August 2022 (Hebrew).

[14] Guidelines to Companies Providing Technological Services to Political Parties, *PPA's website*, 25 August 2022 (Hebrew).

[15] Guidelines for Training Employees/Volunteers During Election Campaign, PPA's website, 25 August 2022 (Hebrew).

[16] Supreme Court Ruling 1311/20 Adv. Shahar Ben-Meir v. Likud, *Nevo's website*, 25 February 2020 (Hebrew).

10(c) The Registrar shall supervise compliance with the provisions of this Law and the regulations thereunder.

10 (e1) (e1) In carrying out his functions, an inspector may:

(1) demand every relevant person to deliver to him information and documents relating to a database;

(2) enter a place as to which he has reasonable belief that a database is being operated, search the place and seize objects, if he is convinced that doing so is necessary to ensure implementation of this Law and to prevent violation of its provisions; the provisions of the Criminal Procedure (Arrest and Search) Ordinance [New Version], 1969 shall apply to an object that has been seized under this section; arrangements for entering a military installation or an installation of a security authority within its meaning in Article 19(c) shall be determined by the Minister of Justice upon consultation with the minister in charge of the security authority, as the case may be; in this paragraph, "object" includes computer material and output as defined in the Computers Law, 1995.

(3) notwithstanding the provisions of paragraph (2), an inspector shall not enter a place that is used solely as a residence, other than pursuant to an order given by a judge of the Magistrate's Court.

21. Therefore, Zulat proposes that the PPA take the following preemptive steps:

a. Require political parties to notify it in advance of all the outsourcing companies hired to provide them services that are relevant to the provisions of the Privacy Protection Law.

b. Require political parties and their service providers to submit detailed statements about their compliance with the relevant provisions of the law and PPA directives, as well as the precautions they have taken to avoid their violation. Thus, the parties would be required to declare that the PPA's directives regarding their obligation to conduct a preliminary examination of the compatibility of applications and providers with the provisions of the law had been carried out, in accordance with Articles 5, 15, and 16 of the Protection of Privacy Regulations[17] and Directive 2011/2 of the Registrar of Databases[18] (similar to the Defense Export Control Agency's guidelines regarding the obligation of exporters to submit declarations and fill out questionnaires[19]).

c. Require parties and service providers to appoint a "privacy protection officer" (similar to a "compliance officer"), who would be in constant contact with the PPA and would be responsible for regularly overseeing internal compliance with the provisions of the Privacy Protection Law and the PPA's directives.

d. Set up a hotline to field real-time complaints from the public about violations of privacy and forward them to the relevant authorities.

[17] Protection of Privacy Regulations (Information Security), 2017, *Nevo's website*, 14 November 2021 (Hebrew).
[18] Directive 2011/2 of Registrar of Databases, *Law, Information, and Technology Authority's website*, 7 June 2012 (Hebrew).
[19] Instructions for End Use/User Certificate, *Defense Ministry's Defense Export Control Agency's website*, 15 May 2014.

e. Publish short and easy-to read pamphlets ("Rights at a Glance") to increase public awareness, acquaint the public with its rights, and spell out the do's and don'ts of political parties in the run-up to an election.

Insofar as the PPA believes that the extensive provisions of Articles 10(c) and 10(e1) of the Privacy Protection Law are insufficient to enforce proposals a, b, and c unless new regulations are issued, it could introduce them as "best practice" likely to help the parties and service providers to ensure compliance with their obligations not to violate the privacy of citizens and to safely and properly secure information.

Protecting the privacy of Israel's citizens during the run-up period is imperative and critical for upholding a free and fair election.

I would appreciate your comments. Best regards,

Einat Ovadia

Executive Director of Zulat for Equality and Human Rights