22 April 2024, Brussels

For the attention of Vice-President of the European Commission Věra Jourová,
CC/ Cabinet of European Commissioner for Justice

Re: Concerns Regarding European Commission's Reconfirmation of Israel's Adequacy Status in the Recent Review of Adequacy Decisions

We, a coalition of civil society organisations dedicated to safeguarding digital rights, wish to voice our concern regarding the decision made by the European Commission regarding its review of 11 existing adequacy decisions, specifically in this letter the adequacy decision with Israel made public on 15 January.

The Commission has opted to uphold these Adequacy decisions, which permit the unrestricted transfer of data to specific jurisdictions. In these decisions, the Commission must comply with the principles and conditions outlined in the *Schrems I* and *Schrems II* judgments of the Court of Justice of the European Union (CJEU) when evaluating the Adequacy of non-EU countries. This is crucial to ensure the legality of onward transfers of individuals in the EU's personal data. Following a comprehensive examination of the information presented by the Commission and other relevant documentation, we are concerned about the inclusion of Israel in the list, in particular, because the country's regulations regarding the obtaining, processing and onward transfer of personal data do not align with the standards outlined in the GDPR and the EU Charter of Fundamental Rights (Charter) as interpreted by the CJEU. While the content of this letter focuses on the inclusion of Israel in the reviewed decisions, we are also examining potential inadequacies concerning other countries on the list.

We therefore **request clarification from the Commission on six pivotal matters crucial to the Adequacy decision framework**: first, the rule of law in Israel; second, the scope and substance of Israel's current and future privacy and data protection legal framework; third, the role of national security provisions and entities; fourth, onward transfers beyond Israel's internationally-recognised borders; fifth, the review procedure; and sixth, the application of the Adequacy framework in the context of Israel's involvement in what the United Nations High Commissioner for Human Rights called a 'catastrophic' ongoing situation in Gaza, and which is the International Court of Justice (ICJ) has found to be a plausible case of genocide, following the case brought to the court by South Africa, and for which it has already issued six provisional measures .

Firstly, we question whether Israel's current rule of law context enables the country to provide an adequate level of data protection, the key prerequisite for an Adequacy decision. The Commission temporarily halted the review process last year due to concerns about both the rule of law and data protection in Israel. **The International Bar Association has highlighted that the rule of law in the country has been under threat,** mainly due to actions by the current government, attempting controversial judicial overhaul that may significantly jeopardise, amongst others, the independence of the judiciary and division of power. The implications of these reforms were so alarming that Eran Toch, a senior member of the Israeli Privacy Protection Council, resigned in July 2023 amid concerns over the maintenance of the country's Adequacy status. Whilst Israel's Supreme Court has issued two judgments which address some of these threats in early January, the fundamental **dilemma about the court's power to conduct judicial review and determine the ultimate authority in the legal system** remains. With these being pivotal aspects for the protection of the right to personal data, we are concerned that the Commission has not sufficiently taken these developments into account.

Secondly, Israel's privacy and data protection framework is still not sufficiently aligned with the GDPR. While we do recognise that this adequacy was adopted under the EU data protection

framework that preceded the GDPR, the Commission underlined in its report that you fully took into account the entry into application of the GDPR in the EU when rechecking the essentially equivalent protection offered by Israel. The Israeli data protection law, dating back to 1981, differs significantly from the GDPR. In 2022, Israel indicated its intention to update its data protection framework with the 2022 Privacy Protection Bill amending the Protection of Privacy Law, currently being discussed at the Knesset. Because the text has not been adopted yet, the framework has been updated by the Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area) 5783-2023, and guidelines issued by the Privacy Protection Authority. However, despite anticipation of modernisation aligned with Council of Europe Convention 108 and the amending Protocol, creating the modernised Convention 108+ standards following the 2011 Adequacy decision, these updates **only offer a partial alignment with GDPR definitions, standards and spirit** regarding critical issues such as the accountability principle, the legal basis for data processing, and the criteria that have to be met for the consent of data subjects to be valid. While some GDPR aspects have been addressed, and the framework presents some improved data protection standards and procedures, as mentioned in the Country reports, there is still a gap between the current level of data protection guaranteed by Israeli law and the standards necessary for ensuring adequacy with the EU. For that, 'essential equivalence' with the GDPR is required (*Schrems I*). We thus need clarification on the Commission's benchmarks and evaluation process, notably when it comes to the acknowledged room for improvement regarding legal certainty and solidification of the protection of personal data.

Thirdly, the Commission's decision seems to overlook that **Israel's national security legislation appears to conflict with EU standards on necessity and proportionality, particularly regarding the country's use of bulk data powers or surveillance operations,** which have been criticised by human rights experts. We hereby express concern about the Israeli privacy and data protection framework failing to prevent undue access to data by Israeli law enforcement and security agencies. Such access is characterised by a lack of robust standards that effectively safeguard fundamental rights and ensure accountability and transparency in data handling. In the *Schrems I* ruling, the CJEU emphasised that unrestricted access by intelligence authorities to the content of electronic communications contravenes Article 7 of the Charter. It also noted that the United States failed to offer adequate legal remedies for non-US individuals affected by mass surveillance, contravening Article 47 of the Charter. Similarly, mass surveillance programs operated by Israel, as well as targeted surveillance without judicial permission or supervision, seem inconsistent with the principles of necessity and proportionality and fall short of meeting the standards set by EU data protection law and the Charter, as interpreted by the CJEU.

The Commission's assessment fails to consider **Israel's surveillance practices, displaying an inaccurate and limited understanding of the types of communications data - including data on communications between individuals in the EU - falling under Israel's data retention and lawful interception powers**. The initial 2011 Adequacy decision did not consider government access to personal data, and the Country Report mentioned herein above provides only a cursory examination of Israel's national security laws. We are concerned that the Commission does not question the lack of independent oversight of communications interception authorisations. Although there are instances where Israeli law enforcement agencies undergo *ex-ante* judicial review for metadata acquisition, there are notable distinctions in the regulations governing the Israel Security Agency's acquisition, processing, and retention of metadata. In this context, the use of data obtained requires authorisation solely from the Agency director, and the guidelines pertaining to the use, retention, security, and processing of this data are established by the Prime Minister and are classified. In December 2023, a proposed measure (in combination with a temporary order also posing concerns from a data protection perspective) outlined a notable extension of the Agency's authorities proposing to establish a legal foundation for employing advanced surveillance tools, akin to NSO Group's Pegasus, and also enabling the Agency to clandestinely access and collect data from diverse biometric databases and cameras within Israel (data that was allegedly unlawfully shared in the past, moreover). In its *La Quadrature du Net* ruling, the CJEU emphasised that

according to the Charter, intelligence agencies' access to data must be grounded in a publicly accessible law that explicitly outlines clear and stringent restrictions on such access.

Moreover, the Country Report's discussion on metadata collection omits commentary on **'bulk' practices,** merely stating that it is requested 'where necessary'. The Commission overlooks the fact that Israel lacks data retention provisions, as all communications metadata are transferred directly to the Israeli Security Agency instead of being retained by service providers for future access. Exacerbating the situation, it remains unclear whether individuals in the EU will have access to an independent and impartial redress mechanism concerning the collection and use of their data by Israel's Security Agency. It is also uncertain whether the Israeli regulatory framework includes sufficient safeguards for accessing data transferred under the framework in relation to national security purposes.

Last but not least, any Adequacy framework must uphold data subjects' **rights of access and to be informed about the recipients of their shared data**. Unfortunately, this has not been the situation for EU citizens affected by targeted surveillance operations involving NSO Group's Pegasus spyware. Requests to the Israeli government for information on NSO Group's clients have gone unanswered, despite its knowledge and authorisation of such sales through granting export licences to spyware companies. This has been stressed in the European Parliament's PEGA Committee report. Moreover, individuals in the EU appear to lack various legal remedies, such as free independent dispute resolution mechanisms and mediation services, in case their data are inaccurately processed by Israeli companies or may have been accessed by Israeli security agencies.

Fourthly, we are concerned that **the renewal of Israel's Adequacy status could result in circumventing EU rules regarding transfers to territories not deemed adequate under EU law**. We consequently advocate for meaningful respect of the 'territorial clause,' aligning with the EU's 'differentiation policy.' This policy distinguishes between the recognised State of Israel within its 1967 borders and the Occupied Palestinian Territory (oPt) - as well as the occupied East Jerusalem and Golan Heights, both illegally annexed by Israel - in accordance with UNSCR 2334 and CJEU judgement *Firma Brita GmbH v Hauptzollamt Hamburg*. This is crucial considering what the UN has highlighted as constituting a prolonged, gradual informal annexation of the oPt over decades. While the 2011 Adequacy decision for Israel explicitly pertains to the internationally recognised borders, a study by Douwe Korff, a human rights and data protection expert, suggests that Israeli legislation, even the most recently updated, does not make such a distinction. It seems, therefore, that Israel **does not treat onward transfers of data (including EU data) from Israel to the oPt as transfers abroad**. Moreover, the 2022 Privacy Protection Bill amending the Protection of Privacy Law and complementary legislation (including case law), as well as the guidelines provided by Israel's Privacy Protection Authority, fail to offer clarity regarding the extraterritorial application of the text.

These concerns have been heightened by the discoveries made about **the role of Israel's intelligence agencies during the war on Gaza**. For years, Israel has exerted control over access to telecommunications and the internet throughout the entire oPt. This control has enabled Israel to engage in both mass and targeted surveillance, collecting data that feed mass biometric databases containing information of Palestinian residents in the oPt and most likely contributes to the database used by an artificial intelligence system which generates potential airstrike targets in the current attacks on the Gaza Strip, which UN experts have labelled as crimes against humanity,and give "reasonable grounds to believe that the threshold indicating the commission of the crime of genocide…has been met.", by the UN Special Rapporteur on the situation of human rights in the Occupied Palestinian Territories. It is very concerning, when considering that transfers to the country in question will be assimilated to intra-EU transmissions of data, that the Commission's Israel Country Report on the Adequacy decision's functioning does not address Israel's adherence to the territorial limitation. We urge the Commission also to shed light on this issue.

Fifth, we are alarmed by the procedural shortcomings observed in the Commission's decision-making process across the whole set of Adequacy review decisions announced in January. Acknowledging that this is a review of an existing Adequacy decision adopted under Directive 95/46/EC, considering the specifics of the context, we nonetheless emphasise the **importance of stakeholder input**. The Commission's report on the review asserts that 'the Commission services gathered the views of [...] the GDPR Multi-Stakeholder Expert Group (which includes representatives of civil society, industry, academia, and legal practitioners) on the progress of the evaluation', but to our knowledge, this has not been the case. **We urge the Commission to provide detailed insights into the process utilised for collecting stakeholder feedback.**

Sixth, when making Adequacy decisions, and as specified in Recital 101 to 107 and Article 45 of the GDPR, **the Commission should, in its assessment and review of the Adequacy decision, take into account criteria such as 'how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards'**[1]. Even though, as mentioned above, we are aware that this was a review process of a decision adopted under Directive 95/46/EC, we also need to emphasise that **the operation should still encompass a thorough assessment of the laws and practices of the concerned country.**

In January, the International Court of Justice (ICJ) held a public hearing in which South Africa argued that Israel is committing genocide in the Gaza Strip, with the ICJ ruling on provisional measures indicating that South Africa's claim is plausible. Highlighting the 'catastrophic humanitarian situation' in Gaza, the Court stressed the 'urgency' and 'real imminent risk' of irreparable harm to Palestinians. Consequently, the court ordered legally binding provisional measures, placing a duty on the EU and its Member States to ensure their implementation. These measures are expressly relevant to the protection of fundamental rights, the rules-based international order and the rule of law, and therefore have an important bearing on any Adequacy decision. **The current context in Israel and the oPt seems to have exacerbated the disregard for the rule of law, particularly concerning the processing of personal data for national security purposes and is, therefore,** an important consideration for possible (in)adequacy. We seek to understand why the Commission did not halt the process given the gravity of this context and its relevance to Adequacy and the consequent protection of individuals in the EU's data protection.

All in all, we conclude that **the inclusion of Israel in the adequacy review list warrants further scrutiny and clarity**. We urge the Commission to address these concerns with transparency and accountability to understand if this decision should be revoked. **The Commission must ensure that Adequacy decisions and their review provide a solid, sufficient, and future-oriented legal basis for data transfers and that all Adequacy decisions are deemed acceptable upon scrutiny by the CJEU,** in line with all the points mentioned throughout this letter. In this regard, we are in the process of examining the content and procedures of other renewed Adequacy decisions and advocate for further dialogue and engagement to ensure that the rights and interests of all stakeholders and rights-holders are adequately protected in all data transfers.

We remain at your disposal for any questions you may have.

Yours sincerely,

Signatories

1 in line with Article 2 of the Euro-Mediterranean Agreement establishing an association between the European Communities and their Member States, of the one part, and the State of Israel, of the other part, whereby '*Relations between the Parties, as well as all the provisions of the Agreement itself, shall be based on respect for human rights and democratic principles, which guides their internal and international policy and constitutes an essential element of this Agreement*'

EDRi European Digital Rights
Access Now
Politiscope
Homo Digitalis
IT-Pol Denmark
Bits of Freedom
European Sex Workers' Rights Alliance - ESWA
Statewatch
Vrijschrift.org
Amnesty International
SHARE Foundation