Date 24-06-2025

Re: Continued Lack of Response on Israel's Adequacy Status and Urgent Need for Reassessment in Light of New Developments

For the attention of Michael McGrath, European Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection

A year ago, a coalition of civil society organisations dedicated to safeguarding digital rights voiced our concern regarding the European Commission's decision to reconfirm Israel's data protection adequacy status in its review of 11 existing adequacy decisions, as communicated in a letter dated 22 April 2024. Since then, Israel's legal and political trajectory has only deepened our concerns, including the adoption of new laws undermining independent oversight, escalating human rights violations in Gaza, and the continued erosion of the rule of law and judicial independence. The combination of legal reforms, unchecked intelligence access, and the operational deployment of EU-linked data in repressive practices further undermines the credibility of Israel's adequacy status. It has now been more than a full year since we first raised these issues, and we deeply regret that neither our concerns nor those raised by other civil society organisations and representatives have been addressed. This continued failure to engage not only undermines transparency but also raises serious questions about the European Commission's commitment to upholding the General Data Protection Regulation (GDPR) and protecting fundamental rights.

In January 2024, the Commission 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 outward and onward transfers of personal data for individuals in the EU. Given the Commission's lack of reaction, we are still extremely concerned about the inclusion of Israel in the list. Firstly, this is because, as we argued in our previous letter, 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. Secondly, this isbecause of Israel's ongoing actions in Gaza, which the International Court of Justice (ICJ) preliminarily ruled can plausibly be regarded as genocide, which has an impact on whether a country's data protection regime can be considered adequate. Since then, Israel's actions have intensified, with the UN Special Committee reconfirming in November 2024 that the warfare methods are 'consistent wit

h genocide'. Personal data are used to facilitate these criminal actions, including indiscriminate killings, as explained in the Annex below.

While the content of this letter focuses on the inclusion of Israel in the decisions reviewed by the Commission, we are also examining potential inadequacies concerning other countries on the list, and have been vocal about other decisions such as the UK and the US.

In April 2024, **we requested clarification from the Commission on six pivotal matters crucial to the Adequacy decision framework,** several of which were echoed - directly or indirectly - in the EDPB Letter to the European Commission on its review of its eleven adequacy decisions adopted under Directive 95/46/EC. These issues are:

1. the rule of law in Israel;
2. the scope and substance of Israel's current and future privacy and data protection legal framework;
3. the role of national security provisions and entities;
4. onward transfers beyond Israel's internationally-recognised borders;
5. the review procedure; and
6. the application of the Adequacy framework in the context of Israel's involvement in what the United Nations High Commissioner for Human Rights has called 'grave breaches of international law committed over the past year and a half'. Respect for international law is a precursor for any state to be deemed adequate for the processing of personal data.

Since the last letter, ongoing and new developments have further demonstrated the urgent need for the European Commission to reassess its position on Israel's adequacy status. Israel's digital sector accounts for approximately 20% of its economy, and a wide range of companies operating in Israel process EU personal data across multiple sectors. Consumer-facing platforms such as Waze (navigation), MyHeritage (genetic testing), Payoneer (cross-border payments), WalkMe (user analytics), Wix (website hosting), and AppsFlyer (mobile marketing) handle sensitive categories of data originating from EU users, including geolocation, biometric and genetic information, financial records, and behavioural profiles. The issue is not that these companies exist, but that Israel's legal framework does not provide enforceable protections equivalent to those in the EU. There are no effective guarantees that EU personal data handled by these

companies will be shielded from access by Israeli security services, especially given the country's sweeping national security exemptions and weak oversight mechanisms (see Annex below). In parallel, surveillance technology firms such as Cellebrite, Cognyte, and NSO Group operate within the same regulatory ecosystem and maintain close ties with the Israeli state. This creates a structural risk of unlawful access, repurposing, or onward transfer of EU data without transparency, accountability, or redress. The GDPR's Adequacy framework rests on the principle of 'essential equivalence' in legal protection. When companies benefit from access to EU data, but operate under a regime where national security interests routinely override privacy rights and where oversight authorities lack independence, that principle is no longer upheld. The Commission's failure to recognise and address these systemic deficiencies renders its adequacy finding unsound, both legally and ethically.

The European Commission's continued silence in the face of these urgent concerns is untenable. The absence of any meaningful response undermines trust in the EU's commitment to fundamental rights and erodes confidence in its data protection framework. We therefore expect a swift and comprehensive response from the Commission on this matter. Failing that, we will seek remedy through the appropriate oversight mechanisms, including the European Ombudsman.

In light of these escalating concerns, we call on the European Commission to urgently:

- Immediately provide a detailed response outlining the legal and factual basis for Israel's continued adequacy status, including whether any new safeguards or oversight mechanisms have been put in place.

- Undertake a full legal assessment of EU-Israel data transfers, ensuring that they do not contribute to mass surveillance, repression, or other practices that violate international law. This should include an immediate review of whether transfers of personal data from EU-based companies to Israeli intelligence and security agencies are taking place in a manner inconsistent with the GDPR and fundamental rights.

- Conduct an urgent reassessment of Israel's adequacy status in light of the ICJ's advisory opinion and the EU's legal obligations to ensure it is not complicit in maintaining an unlawful situation.

- Engage in a transparent dialogue with civil society organisations and independent experts to ensure that the EU's data protection policies are fully aligned with fundamental rights and international law.

The European 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 can withstand scrutiny by the Court of Justice of the European Union. In the case of Israel, this requires confronting how the state's unlawful occupation of Palestinian territory directly undermines the foundational elements of data protection adequacy. Israeli authorities apply their domestic data protection law extraterritorially to the occupied Palestinian territory (oPt), a legal fiction that violates the EU's own differentiation policy and international law. This not only erodes the territorial scope and legal certainty required under Article 45 GDPR but also facilitates access to EU personal data by institutions operating in illegally annexed areas and in support of repressive practices. Moreover, the absence of independent oversight, redress mechanisms, or effective limitations on national security access within these territories means that data subjects cannot meaningfully exercise their rights. This is not a marginal concern: surveillance and biometric data systems such as Blue Wolf and Red Wolf are deployed in occupied areas, often with the support of infrastructure and institutions that blur the boundaries between commercial, security, and military operations. In this context, data transfers from the EU risk being repurposed for use in a context that not only lacks legal safeguards, but actively facilitates systematic rights violations.

If the EU fails to reassess Israel's adequacy decision, it will not only violate its own legal standards but will also risk contributing to the entrenchment of an unlawful situation through the provision of digital infrastructure. The ICJ's Advisory Opinion of 19 July 2024 reaffirmed that Israel's occupation of Palestinian territory is unlawful and clarified that third states, including the EU and its member states, have an obligation not to aid or assist in maintaining that situation. In this light, the EU's endorsement of continued data flows to Israel in the absence of adequate safeguards, territorial limitations, or legal redress risks placing the Union in breach of its obligations under international law. The review of Article 2 of the EU-Israel Association Agreement, as announced by the EU High Representative in May 2025, also underscores the growing recognition that Israel's conduct is incompatible with the human rights commitments binding under EU external relations law.

Failing to reassess Israel's adequacy status does not only risk entrenching the EU's complicity in systematic human rights violations: it also undermines the credibility and legal consistency of the EU's entire data protection framework. The Adequacy mechanism, as foreseen in Article 45

GDPR, must provide a robust and principled basis for ensuring the protection of personal data beyond EU borders. This requires legal certainty, respect for fundamental rights, and alignment with international law. When Adequacy decisions are maintained despite overwhelming evidence of divergence from these principles - as in the case of Israel - the standard of 'essential equivalence' is eroded, and with it, the EU's capacity to credibly demand high standards elsewhere. If the Commission fails to uphold its own criteria, other Adequacy decisions - past and future - risk becoming politically expedient rather than rights-based. This jeopardises the coherence of the GDPR and sets a dangerous precedent that weakens protections for people both inside and outside the EU.

For the signatories, this is a matter of upholding the rule of law and the integrity of the EU's data protection regime. The credibility of the Adequacy framework depends on consistent, principled application. Anything less risks turning a cornerstone of the GDPR into a politically negotiable instrument, with profound consequences for rights, accountability, and global digital governance. This inconsistency is further amplified by the parallel recognition, within the EU's own external policy framework, that Israel's breaches of human rights obligations under the Association Agreement may justify appropriate countermeasures, including suspension.

We look forward to your urgent response to these matters, and remain at your disposal for any questions you may have.

Yours sincerely,

Signatories
European Digital Rights (EDRi)
Access Now
Electronic Privacy Information Center (EPIC)
Alternatif Bilisim
Hermes Center Hacking for Human Rights
Politiscope
IT-Pol Denmark
Annir Initiative
Aspiration
Homo Digitalis
Bits of Freedom
Kawaakibi Foundation
SMEX
European Sex Workers' Rights Alliance (ESWA)
7amleh - Arab Center for Social Media Advancement
Statewatch
Vrijschrift.org

Annex: Background and Basis for Civil Society's Intensified Concerns Over Israel's Data Protection Practices

1. The Rule of Law in Israel

In last year's letter, **we questioned 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.** According to the World Bank, Israel ranked 142 out of 176 countries in the Human Rights and Rule of Law sub-indicator of Fragile States Index in 2023. The rule of law situation in Israel has continued to deteriorate significantly. Both UN experts and the International Bar Association raised serious concerns that Israel's actions threaten the international rules-based order, undermine international law, and weaken the authority of the United Nations. Serious breaches of international law persist. Additionally, there is growing concern about the centralisation of power in the executive, with Prime Minister Netanyahu's government systematically targeting key oversight officials in order to remove institutional checks on the office of the Prime Minister. This power consolidation further undermines democratic governance and legal accountability. The implementation of the so-called 'Deportation Law' in November 2024, which allows for the deportation of certain foreign nationals and could rely on the use of EU citizens' personal data to enforce it, is another alarming development. This law stands in clear contradiction to the international human rights standards that the EU upholds and reinforces concerns over Israel's commitment to data protection principles.

The core issue remains unresolved: Israel's lack of a formal constitution, coupled with the current uncertainty surrounding the court's power to conduct judicial review, highlights a fundamental **'constitutional crisis'. This crisis undermines the legitimacy of the legal system in terms of ensuring the protection of rights, including the right to personal data**. Given the pivotal role that judicial independence and the rule of law play in upholding data protection standards, we are concerned that the Commission has not sufficiently taken these ongoing developments into account in its assessment of Israel's Adequacy status.

Furthermore, the Summer 2025 Knesset session introduces bills that severely restrict freedom of expression, academic freedom, and civic participation, while transferring extensive powers to the executive. This legislative push includes criminalising dissent, expanding police surveillance powers, and politically controlling public media. These moves represent not just a weakening, but a dismantling, of institutional safeguards necessary for data protection and independent oversight.

2. The Scope and Substance of Israel's Current and Future Privacy and Data Protection Legal Framework

Israel's privacy and data protection framework is still not sufficiently aligned with the GDPR. While we do recognise that the original (2011) adequacy was adopted under the EU data protection framework that preceded the GDPR, the Commission underlined in its report that it 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 5741-1981.

On 5 August 2024, the Knesset approved a significant amendment to the law in the form of Amendment 13, the most substantial revision to Israel's privacy framework since the law's initial enactment, which will enter into effect a year as of its publication. Amongst other aspects, Amendment 13 significantly reduces the powers of Israel's data protection authority, the Privacy Protection Authority (PPA) during election periods, raising serious questions about the authority's independence and effectiveness at times when oversight is most crucial. **This and other changes directly undermine compliance with one of the core requirements of the GDPR: the existence of an independent supervisory authority with adequate powers and autonomy.** Therefore, there is still a serious 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. 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.

3. The Role of National Security Provisions and Entities

In our initial letter, we also emphasised that **the Commission's assessment failed to adequately consider the incompatibility between Israel's national security framework and the safeguards required under EU data protection law**, particularly with regard to necessity, proportionality, and effective oversight. The 2011 Adequacy Decision did not examine government access to data, and the 2024 Country Report continued to provide only a cursory treatment of Israel's surveillance architecture. As a new concerning development, Amendment 13 mentioned earlier introduces deeply concerning exceptions in the national security domain including in relation to. agencies such as the Israel Defense Forces (IDF), Shin Bet, and Mossad, who will be subject to separate oversight procedures that will be largely self-managed and shielded from external enforcement.

These bodies will be almost fully exempt from the oversight of the PPA. These exceptions are in direct tension with GDPR principles, and the EDPB explicitly flagged these exceptions as areas that must be closely assessed and monitored in the context of Adequacy decisions.

Pending legislation would give law enforcement sweeping powers to use spyware and conduct covert digital searches. These proposals lack judicial oversight and disproportionately target Palestinians, making any notion of effective redress for EU data subjects in Israel untenable.

The Commission's analysis also disregarded the growing integration of AI and biometric technologies into Israeli surveillance practices, such as the deployment of facial recognition systems like Red Wolf and Blue Wolf in the occupied Palestinian territory (see below). These technologies are used to monitor, restrict, and categorise Palestinian individuals, often in ways that raise concerns of racial profiling and automated decision-making without human oversight. Even more concerningly, these databases are used to feed AI-driven systems such as *Gospel* and *Lavender,* which are ostensibly used to enhance the identification of military objectives and individuals deemed targetable. However, their use appears to contribute to the increasing automation of lethal operations, raising profound ethical, legal, and human rights implications. While there is no conclusive public evidence that personal data from the EU is used to develop or train such systems, the absence of firewalls between commercial data processing and national security access makes this a material risk that cannot be ignored.

The exact same concern applies to the involvement of major technology companies, including Microsoft and Google, in supporting programs that enable the collection and processing of such data. Both companies maintain establishments within the EU and are therefore subject to the GDPR. While there is currently no conclusive public evidence that personal data originating from the EU has been used to develop or train these systems, the lack of robust safeguards separating commercial data processing from potential national security access introduces a material risk that must not be overlooked.

These structural deficiencies are not theoretical. **Data transferred from the EU to Israel under the Adequacy framework is not demonstrably protected from access by Israeli intelligence or law enforcement bodies.** There is no indication that such data, once in Israeli jurisdiction, is immune from being repurposed for national security objectives. Moreover, individuals in the EU whose data is transferred to Israel lack access to effective and independent redress mechanisms. It remains unclear whether any authority exists that can provide impartial adjudication or remedies in cases where personal data has been accessed unlawfully or processed in breach of GDPR-equivalent standards.

A recent incident involving EU representatives brings these concerns into sharp focus. In February 2025, two MEPs were detained and deported upon arrival in Israel, alongside two senior EU civil servants. During their detention, all electronic devices, including Parliament-issued phones and tablets, were confiscated for over 90 minutes. MEP Lynn Boylan has since raised the possibility that her device may have been subject to interference or surveillance and addressed this concern directly to European Commissioner Michael McGrath. As she pointed out, the European Parliament's own IT security services list Israel as a jurisdiction where officials are advised not to bring personal devices due to the risk of state surveillance. This raises a fundamental contradiction: if the Parliament itself considers Israeli authorities a threat to the data security of its members and staff, how can the Commission credibly maintain that personal data transferred under the Adequacy framework enjoys an adequate level of protection?

Last but not least, any Adequacy framework must guarantee that data subjects are able to exercise their rights of access and to be informed about the recipients of their personal data. These are foundational principles of EU data protection law. Yet in practice, and as mentioned in our previous letter, individuals in the EU affected by targeted surveillance operations involving Israeli technologies have been unable to obtain such information.

In light of these deficiencies - both structural and procedural - it is impossible to reconcile Israel's current legal framework with the threshold of 'essential equivalence'. The Commission's failure to fully evaluate these risks undermines the integrity of the Adequacy framework and exposes individuals in the EU to surveillance practices that are fundamentally at odds with EU fundamental rights standards.

4. Onward Transfers Beyond Israel's Internationally-recognised Borders

We also remain concerned that **the renewal of Israel's Adequacy status will inevitably result in circumventing the EU's 'differentiation policy.'** This policy distinguishes between the recognised State of Israel within its 1967 borders and the occupied Palestinian territories (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. Even the aforementioned letter from the EDPB requested a more detailed explanation of the rules on onward transfers in the assessed third countries and how their application in practice had developed. The EDPB explicitly underlined that, in the context of the 11 reviews, the applicable legal framework was in some cases very different from that set out under EU law.

Legal analysis by Professor Douwe Korff reinforces these concerns, concluding that the European Commission's reaffirmation of adequacy effectively ignores both the legal fiction of applying Israeli law in the oPt and the broader international law obligations of the EU. Korff highlights that this approach is incompatible with the duty of non-recognition under international law, and that it risks breaching the EU's own Charter and Treaty obligations by enabling the use of EU personal data in furtherance of an unlawful occupation. He also notes that the Commission's failure to impose clear territorial safeguards facilitates data transfers to actors operating in or from settlements, undermining the legal integrity of the adequacy framework.

While the 2011 Adequacy Decision for Israel explicitly limits its scope to the territory of the State of Israel as recognised by the international community, there appears to be no effective mechanism to ensure this territorial limitation is observed in practice. Some may argue that the extension of Israeli data protection law to the oPt resolves the matter by ensuring that EU data transferred to Israel remains protected, even if further processed or accessed in the oPt. However, this argument is legally unsound. **The application of Israeli law to the oPt does not neutralise the problem - it constitutes it.** Accepting such a legal fiction for the purposes of assessing adequacy would amount to tacit recognition by the EU of Israel's *de facto* jurisdiction over territory which the EU itself, in accordance with international law, does not recognise as Israeli. **It would also directly contravene the EU's obligation under international law** - including the duty of non-recognition of unlawful situations, as codified in the International Law Commission's Articles on State Responsibility - not to aid or assist in maintaining the consequences of serious breaches of peremptory norms, such as the prohibition on the acquisition of territory by force.

This blurring of jurisdictional lines is particularly problematic when considering the operational realities of Israel's governance and surveillance infrastructure in the oPt. For example, the headquarters of both the Israeli police and the Ministry of the Interior are located in occupied East Jerusalem, a territory not recognised by the EU as part of Israel. Similarly, Israel's national surveillance command and control centre - which integrates facial recognition technologies, AI-based monitoring systems, and real-time data flows - is based in the Gilo settlement, which is also located in occupied West Bank. The fact that data processing operations - particularly those tied to law enforcement, biometric surveillance, and national security - are anchored in illegally-annexed territory further undermines any claim that the application of Israeli law in these areas is legally neutral or administratively irrelevant. In the absence of territorial safeguards, there is a tangible risk that personal data transferred from the EU may be accessed or processed within

these facilities, thereby implicating the EU in the extension of Israeli jurisdiction over occupied territory and violating the obligation of non-recognition.

On 19 July 2024, the International Court of Justice (ICJ) issued an Advisory Opinion on the Legal Consequences arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, including East Jerusalem. The ICJ reaffirmed the unlawfulness of Israel's occupation and explicitly stated that third states, including the EU and its member states, have a responsibility to not to contribute to maintaining the unlawful situation created by Israel, and not to recognise its legality or take steps that would imply such recognition. **The ICJ's findings thus make clear that failing to reassess Israel's adequacy status risks putting the EU in direct violation of its obligations under international law.** Human rights organisations, including Amnesty International, have called on the European Commission to conduct a legal assessment of EU-Israel cooperation to determine which aspects may violate international law, and we contend that this should include the renewal of its adequacy decision. The continued absence of such an assessment undermines the EU's credibility in both protecting and promoting human rights and the rule of law.

Furthermore, such a position would place the EU in contradiction with its own GDPR framework. Adequacy decisions are meant to ensure that data subjects benefit from a level of protection 'essentially equivalent' to that provided within the EU - not merely that data is subject to some legal framework in the destination country, regardless of its legitimacy or territorial reach. **Where the application of Israeli law itself is a matter of legal and political contention, its use as a vehicle to justify adequacy over territories beyond Israel's recognised borders renders the framework untenable.** It is not merely a matter of functional adequacy; it is a matter of legal principle.

This concern is not abstract. As noted above, numerous Israeli technology firms operate in or in relation to settlements or other areas of the oPt, including providers of surveillance infrastructure, biometric data services, and AI tools used by the Israeli military and border authorities. In the absence of clear territorial safeguards and enforcement mechanisms, **there is a material risk that personal data transferred from the EU could be processed in occupied territory, or by actors supporting Israel's prolonged occupation.** This would implicate the EU in the normalisation of an unlawful situation and expose data subjects to additional risks that are neither acknowledged nor mitigated by the existing Adequacy framework. The EU's depiction of Israel as a model jurisdictions for data protection, without addressing its well-documented disregard for privacy and data protection rights, effectively normalises mass surveillance practices.

5. The Review Procedure

We also remain alarmed by the procedural shortcomings observed in the Commission's decision-making process across the whole set of Adequacy review decisions announced in January 2024, and **urged the Commission to provide detailed insights into the process utilised for collecting stakeholder feedback.** This concern hasn't been addressed either. In this regard, the EDPB Letter to the European Commission on its review of its eleven adequacy decisions adopted under Directive 95/46/EC further reinforced our concerns. The EDPB highlighted the critical importance of ensuring a transparent and inclusive consultation process, underscoring the need for the Commission to demonstrate how stakeholder feedback is collected, integrated, and reflected in its decision-making. The EDPB's emphasis on procedural transparency strengthens our call for a detailed explanation of the consultation process and reaffirms that the adequacy reviews must include meaningful engagement with all relevant stakeholders to ensure that decisions align with the core principles of the GDPR and protect individuals' rights effectively.

6. Adequacy and the Respect of International Law

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]. The EDPB's letter underscores the urgent need for clarification of this aspect, particularly in point 'I. General Remark.' It specifically calls on the Commission to provide more transparent information on the assessment of these elements in both law and practice, in the context of future adequacy decisions as well as reviews. Nothing in the wording of these provisions suggests that the Commission's assessment should be limited solely to these aspects when evaluating data protection frameworks. Rather, the references to the rule of law, access to justice, and international human rights standards function as broad guiding principles that encompass, but do not exhaust, the range of factors relevant to determining whether a third country ensures an adequate level of protection. **The structure of Article 45 and the accompanying Recitals make clear that adequacy requires a comprehensive and contextual assessment of the legal framework in question, including its substantive and procedural safeguards, enforcement mechanisms, and actual implementation.** Given that data protection is a fundamental right under the Charter of Fundamental Rights of the EU, its adequacy must be assessed in a manner that fully accounts for the evolving risks posed by state and corporate surveillance, cross-border data flows, and the global political economy of digital governance. Confining the assessment to a narrow reading of these criteria would be

incompatible with the GDPR's objective of ensuring a level of protection that is 'essentially equivalent' to that guaranteed within the EU.

In January 2024, the 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, more so when we consider that the war has lasted for at least 18 months, leaving behind more than 53,000 deaths. **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.** While the ceasefire in Gaza may have brought a temporary respite, systematic human rights violations continued. On 18 March 2025, Israel reinitiated and escalated its military operations in Gaza, intensifying mass surveillance, digital repression, and violations of international law, and threatening with permanent occupation of the Strip. Reports indicate that data-driven targeting, biometric surveillance, and other digital technologies are being used to facilitate human rights abuses and systematic oppression. These actions demonstrate how the unregulated flow of data, facilitated in part by the EU's adequacy decision, contributes to ongoing violations. **We still seek to understand why the Commission has not halted 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.**

Last but not least, in the domestic context and in line with the arguments in Section 1, the Israeli government is not only undermining democratic institutions but actively constructing a legal infrastructure that enables authoritarian rule. This includes the systematic erosion of judicial independence, centralisation of executive power, and the enactment of discriminatory laws targeting individuals on the basis of ethnicity and nationality. Such measures are not peripheral. They go to the heart of a legal and institutional environment that is meant to guarantee the protection of fundamental rights, including the right to personal data. Article 45 of the GDPR requires that Adequacy assessments take into account respect for the rule of law, human rights, and effective legal remedies. When a government weakens these safeguards by design, it cannot credibly be considered to offer a level of protection that is essentially equivalent to that of the EU. Endorsing adequacy in such conditions does not just fail to meet the legal standard. It

legitimises a framework that is structurally incapable of upholding the rights of data subjects and of people more broadly.

In parallel to these concerns, we note that the EU has formally initiated a review of Israel's compliance with Article 2 of the EU-Israel Association Agreement, which states that respect for human rights and democratic principles is an essential element of the relationship. This development reflects growing institutional recognition within the EU that Israel's actions may breach the human rights clause that underpins bilateral cooperation. This review could lead to appropriate measures under Article 79 of the Agreement, including suspension. It would be legally incoherent for the EU to maintain Israel's Adequacy status under the GDPR while simultaneously acknowledging that its conduct may violate the foundational human rights obligations of the Association Agreement.