EDRi

European Digital Rights

Feedback from European Digital Rights (EDRi) on "Travel - digitalising travel documents to make travelling easier"

23 December 2024

Introduction:

EDRi is Europe's biggest network of civil society organisations working together to ensure the protection of fundamental rights, as enshrined by the Charter of Fundamental Rights of the European Union ("the Charter") and the wider European aquis, in laws and policies relating to technology and data. As a collection of technologists, lawyers, academics, human rights advocates and other specialists, we welcome the opportunity to share our perspective on the European Commission's (EC's) proposal to digitalise travel documents and create a digital travel credential (DTC).

The focus of this consultation is the '*Proposal for a Regulation establishing an application for the electronic submission of travel data ("EU Digital Travel application") [...] as regards the use of digital travel credentials*' (2024/0670 (COD)) (henceforth "the proposal" or the "the travel app"). Whilst we focus our analysis on this proposal, we note that the majority of concerns raised here are also relevant to the concurrent consultation on the complementary Council Regulation, and ask that they be considered as such.

Whilst we recognise that digitalisation efforts can provide convenience and benefits for people as well as for public administration, it is vital that such efforts are pursued in a transparent and diligent manner. The use of digital technologies frequently entail the processing of personal data, which in the case of this proposal, includes several forms of sensitive data. The use of digital technologies also can have significant environmental impacts, which should be properly taken into account.

Such efforts must also be considered within broader structures of power dynamics between individuals and the state, increasingly hostile border and migration contexts, and risks of discrimination by governments (includingthe risk of exclusion of certain groups and communities as a result of non-inclusive digitalisation programmes).

This is especially pertinent given that the proposal would centralise people's digital travel credentials for visa applications, travel authorisation under ETIAS, the EU Entry-Exit System (EES) and the recently-adopted advanced passenger information (API) Regulation, and would allow for broader use of the DTC via the EU digital identity wallet (eIDAS). These are all laws or proposals about which civil society groups, especially those who work to protect fundamental rights at the intersection of migration and digitalisation, have already raised serious concerns.

EDRi takes the opportunity of this consultation to raise our substantive, evidentiary and procedural concerns about the EC's proposals to digitalise travel documents, based on the claim of making travelling easier. It is our view that the EC has not done their due diligence, and has not properly represented the issues and risks at stake. As such, these proposals may disproportionately limit fundamental rights including, inter alia, privacy, data protection, non-discrimination and freedom of movement. We call into question that claim that travel will be "smoother" as a result of this package.

Our concerns can be split into 7 main parts:

1. **Better Regulation concerns**: Procedural concerns in the context of the EU's Better Regulation commitment, including questions about the legitimacy of the process, the lack of engagement with fundamental rights risks, and the exclusion of inconvenient stakeholders and perspectives;
2. **Exaggerated efficiency promises**: Lack of robustness in underlying efficiency calculations;
3. **Biometric mass surveillance threats**: Obfuscation of the reality and the risks of mass biometric processing and databases;
4. **Convenience for some, profiling for others**: Entrenching systems of surveillance, securitisation and discrimination against people on the move;
5. **Consent and the risk of coercion**: Concerns about how freely-given consent to the DTC would actually be;
6. **Limitations that cannot be solved by an app**: Interrogating the underlying political, technical and economic motivations;
7. **Lucrative digital innovation at the expense of the planet:** The foreseeable scope creep of the DTC, as well as lack of engagement with climate impacts.

This submission has been co-drafted by Ella Jakubowska, Head of Policy, EDRi, and Jesper Lund, Chairman, IT-Political Association of Denmark. We are also grateful to Dr. Derya Ozkul, for providing advice on our submission.

1. Procedural concerns in the context of the EU's Better Regulation commitment

1.a) Concerns about the democratic legitimacy of the process

Firstly, we raise concerns about the democratic legitimacy of the proposed Regulation which – rather than assessing a need and proposing legislation to fill the gap – seems to have started with the International Civil Aviation Organization (ICAO) standards into which the Commission has already funded pilots (see p.4 of the Explanatory Memorandum (EM) and Recital (3) of the Proposal). As explored in the Impact Assessment (IA), *all* policy options considered would rely on this "existing international technical standard" (as noted in EM p.11), making it a foregone conclusion.

By using the proposed Regulation to codify an investment that has already been made, the Commission risks short-circuiting the democratic process – in effect, asking the co-legislators to "rubber stamp" the Commission's wishes. Increasing our concern is the fact that in relation to these ICAO pilots, the Explanatory Memorandum claims "the *indisputable* added value of incorporating the use of digital travel credentials to cross-border travel" (italics for emphasis). This statement exemplifies the unbalanced tone of the overall impact assessment, EM, and proposal, all of which seem to exaggerate the purported benefits of the proposal whilst downplaying the possible risks.

1.b) Lack of diligent engagement with fundamental rights risks

We are concerned that the Commission has not taken seriously the potential impact of the proposal on fundamental rights. We have questions, therefore, about whether the conclusion of the impact assessment is robust.

The context of travel is one of the situations at which the imbalance of power and control between the individual and the state is at its highest. This is particularly profound for those without the privilege of Schengen/visa-free travel, i.e. third-country nationals.

Cross-border travel, by definition, involves the processing of sensitive data, which always entails a limitation on fundamental rights; the question is whether or not a specific act of processing is legitimate, necessary and proportionate to the aim, in light of Article 52(1) of the Charter. However, the impact assessment states on page 39:

> "*The obligation to include the facial image of the holder does not adversely affect the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter, as the information provided by the facial image does not, in itself, make it possible to have an overview of the private and family life of data subjects*."

This statement is a misrepresentation of the assessment of the proposal's limitation on fundamental rights and whether it is proportionate. Article 52(1) of the Charter requires all limitations of fundamental rights to respect the essence of those rights. However, the mere fact that the *essence* of a right has not been violated does not entail either that the rights have not been (possibly unduly) restricted, nor that the rights have been respected. This assessment in the Impact Assessment is therefore a non-sequitur. Going further still, the IA states on page 40 that:

> "*In terms of impacts on fundamental rights other than the right to privacy and the protection of personal data, none of the options would affect the protection of fundamental rights negatively.*"

The Explanatory Memorandum even claims that other than a proclaimed benefit on the right of freedom of movement, "[t]he proposal has limited impact on the protection of other fundamental rights" (p.13). As we will explore throughout this submission, however, the proposal could entail a negative impact on several other fundamental rights. Further issues with the integrity of the assessment made in the IA – particularly the misleading claims about the processing of biometric data - are explored in section 3.

The Impact Assessment (p.40) also admits that:

> "*Some persons may be unwilling or unable to use a DTC due to personal reasons, low IT literacy, disabilities or e.g. not owning a device necessary for its use. Each policy option would allow persons to undergo border checks within the current framework and they too would potentially benefit from shorter waiting times, due to the fact that others have opted in to use the DTC, freeing up capacities and shortening queues at border crossing points. Therefore, the principles of non-discrimination and inclusivity are respected in each policy option*."

Regardless of whether or not these issues *unduly* infringe on rights to equality and non-discrimination (although we will argue in Section 4 that they do) this is still a clear example of those rights being affected – contrary to what the impact assessment claims. We will also explore the impact of the proposal on other rights, such as freedom of movement and the right to asylum, which we also argue are limited by the proposal.

1.c) Non-representative consultation and dismissive attitude towards concerns raised

On p.8 of the Explanatory Memorandum, the Commission explains that a wide range of "concerned stakeholders" were proactively consulted. However, they do not report any direct consultations with civil society organisations, in particular those representing digital human rights and/or the rights of people on the move.

The Memorandum also states that "[m]ost stakeholders expressed wide support for the initiative" (p.8), before contradictorily admitting that in the public consultation, which attracted 7000 respondents, "opinions were largely negative" (p.9). The former claim is, therefore, dubious. The EM further explains that "[a]s motivations for the lack of interest in uptake, respondents highlighted primarily data protection and privacy concerns, as well as overall satisfaction with the current processes" (p.9). However, these concerns are not, as we explain elsewhere in this submission, sufficiently accounted for anywhere in the Commission's proposal or explanations. Instead, as mentioned in the previous section, the EM and IA are overwhelmingly positive about the proposal and its supposedly "indisputable" benefits.

The Commission also dismisses the credibility of letters received in response to the public consultation, which they explain all followed a standard format (EM p.9), and even speculatively suggests that a targeted campaign could be involved. No data are provided to support this claim, despite it being used to justify the dismissal of concerns and of negative feedback. According to Annex 2 of the Impact Assessment (p. 57), the replies came in consistently over the entire runtime of the survey, which the Commission admits there does not indicate a campaign. , Either way, we strongly argue that even if a specific campaign has allowed individuals to express their concern with digital travel documents through a standardised letter, this does not diminish the validity of the concerns raised.

To the contrary, the fact that a high number of individuals mobilised to sent letters to the Commission would show the strength of opinion of these stakeholders.

Instead, the Commission points to the more positive Eurobarometer survey, in which more than 1 in 4 respondents still had a critical response to digital travel documents

(EM p.9) – approximately 6800 people. The fact that the critical respondents were in particular older people and people with low levels of education further emphasises the potential risk of digital exclusion and discrimination against certain categories and communities of people entailed by the proposal. The app will also only be available to those with a chip in their passport (EM p.11); this will mean that nationals of the several dozens countries that do not offer these passports will be entirely excluded from being able to use the system.

Through the questions asked, a Eurobarometer survey also allows the Commission to control the narrative to much greater extent than a public consultation, e.g. by focusing on the potential for faster border procedures, rather than the new data protection risks created by centralised storage of passport data, including facial images. Moreover, a Eurobarometer survey only covers people living in the EU, which excludes third-country nationals living outside the EU who are also affected by the proposal – but whose rights seem to be systematically set aside by this proposal.

The consultation process thus demonstrates a deliberately selective and biased use of data by the Commission in support of their proposal, which downplays and at times even dismisses the genuine and meaningful concerns about its impact (e.g. risks for data protection). Given the nature of these concerns, it is even more surprising that the Commission did not specifically consult with digital rights groups.

2. Lack of robustness in underlying efficiency calculations

One of the main claims justifying the DTC proposal is that it will increase efficiency. It explains that border checks require border personnel to supervise them, even in the case of e-gates, whereby “a border authority official is required to supervise the process” (EM p.2).[1]

However, the proposal does not eliminate the supervisory role of this border authority official – it moves it to a different stage in the process, before the person arrives at the airport or other transport hub. The supposed ‘barrier’ for the traveller is therefore removed from the physical border, but transferred to the preparatory stage. The amount of time saved (about 20 seconds at the border check, according to the data presented in Annex 4 of the Impact Assessment) is simply moved to the person’s hand – and, as we explain is section 6, increased vastly due to the time needed to undertake a ‘liveness check’.

[1] As an aside, we also take this opportunity to note that whilst privacy and data protection are fundamental rights, efficiency and convenience are not, a factor that the European Commission seems not to have taken into account in its Impact Assessment.

For persons with low levels of digital literacy, with buggy smartphones, or with certain physical or mental disabilities, the amount of time it would take them could be significantly longer than that, a possible discrimination issue that the proposal does not account for. And for those choosing not to use the app, they could also face significantly longer delays, as we will explore in Section 5.

The suggestion that fewer border guards would mean more capacity for border authorities is also a non-sequitur. By the proposal's own admission, the same checks will still need to be done, which will require personnel – and they will simply do the checks without the person in front of them. But they will still have to perform the checks – and in fact, these checks may take new forms, again casting doubt on the claim of freeing up border agents.

As noted above, border personnel will also be required to oversee the use of the DTC *as well as* to oversee the use of alternative methods, notably e-gates and analogue border control gates. Border personnel will be needed to assist persons whose travel credentials are not recognised by the automated gates, for example when the facial recognition check fails.[2] Manual supervision of the automated gates is also needed to guard against biometric spoofing attacks, such as the use of latex masks to assume the identity of another person.

The proposal's 'efficiency' calculations are based only on a perfunctory and superficial conception of efficiency as speed and convenience – and even then, the underlying assumptions require careful scrutiny. Additionally, this is not representative of the full picture – with questions of the cost of the system, accuracy of the system, and drawbacks for those unable or unwilling to use the system not sufficiently addressed or balanced against the claimed benefits.

The cost of the system is also significant: as stated in the Explanatory Memorandum, the set-up costs will be 55,600,000 EUR, with an ongoing maintenance cost of 6,200,000 EUR per year for maintenance. Each Member State will also have to make an investment in their infrastructure. Such a significant investment would need to be carefully considered by the co-legislators and properly justified.

Lastly, another concerning justification sits at the heart of the Digital Travel documents proposal: the claim that document fraud at the EU's borders is a problem which justifies the investment in this system – citing "over 17 000 fraudsters" in 2023 alone (EM p.3). However, the EM also notes that there were 593 million border

[2] Moreover, this problem is likely to increase since the future automated gates involve 1:N facial image comparisons, whereas the current e-gates do 1:1 comparisons with a lower error rate (if the same matching threshold is used in both cases).

crossings that year. If we assume for demonstrative purposes that each ‘fraudster’ made 3 crossings during the year, that would still only amount to 0.009% of overall crossings. The scale of this issue therefore does not provide adequate justification for the proposal.

3. Obfuscation of the reality and the risks of mass biometric processing and databases

The proposal highlights as one of its justifications “recent developments [...] in the capabilities and reliability of facial recognition” (Recital 3). Whilst this claim is a constant refrain of industry, reliable data proving that facial recognition works reliably ‘in the wild’ (i.e. not in laboratory conditions) is still scarce. What’s more, given the travel volumes stated in the proposal for 2023 (593 million external border crossings), even a hypothetical system with a precision rate of 99.9% would amount to half a million false negatives a year.

Perhaps most concerning in the context of biometric mass surveillance is the fact that the proposal creates a series of facial image databases and uses them to perform biometric identification, whilst not disclosing these parts of the process in the proposal’s Articles or Recitals. To the contrary, both the Impact Assessment (p.38) and Explanatory Memorandum expressly claim that no new forms of biometric processing will occur:

> “*The proposal does not envisage the creation of a new database. Data subjects therefore remain in control of their own data and choose if and when to use it. If the person chooses to use it for an advance check and facilitated travel, they can submit it, via the application developed and operated by eu-LISA, to the responsible authorities” (*EM p. 13*)*

This claim of the absence of new processing methods or databases is used to argue that the proposed safeguard – that the person remains in control of their data – is sufficient from a rights point of view.

As explained in Recital (7), to create their Digital Travel Credential, a person must perform biometric verification using their passport’s biometric chip, mobile phone and face. Without recourse to any central database, the app would use facial recognition technology to verify that the individual is the same person as in the passport. This form of processing is in theory equivalent in nature to that of e-gates, although in lieu of the local 1:1 matching of facial images on the e-gate, we note that the biometric data is submitted via the internet to a central server (the eu-LISA backend validation service), which creates additional data protection risks. In this step, the system would also collect data on the person’s trip, within the bounds of what is necessary (Recital (8)).

However, where the Commission’s rationale falls down is the following (EM p.13):

> “*To use the digital travel credential, the submitted digital travel credential submitted by the user must be temporarily stored in a local database in the responsible Member State. This temporary database/gallery would be populated with the facial images that are contained in the submitted digital travel credentials. This is necessary to biometrically match the traveller to the submitted digital travel credential when they present themselves at the border-crossing point.”*
>
> *“This entails a one-to-few match, with a view to verifying the identity of the person, as opposed to the one-to-many biometric matching needed to identify an individual. Once the border check has been carried out, the data should be deleted from the temporary database – similar to what is currently done when reading chip data from physical travel documents during border checks.*”

The fact that the databases mentioned enough are “local”, “temporary” and “should be deleted” after the check does not change the substantive fact that these are new databases – making the earlier claim in the IA that the “proposal does not envisage the creation of a new database” demonstrably untrue. The narrative that this is a “gallery” further tries to use language to make the system sound more benign than it really is.

The EM page 13 compares these “temporary” databases to what is currently done when reading chip data from the physical travel document during border checks. However, this comparison is highly misleading because the biometric data processed today is immediately discarded, whereas facial images in the new system will be stored in a central database by Member States’ border authorities between the time of DTC submission through the eu-LISA app and the actual border check. Passengers may submit this data several days before arriving at the border-crossing point.

The use of the term “one-to-few match” is equally troubling. This relates to semi-technical discourse around facial recognition, whereby the terms “one-to-one” and “one-to-many” are sometimes used to distinguish between the former – systems of biometric verification without any central processing – and the latter – systems of biometric identification which rely on central processing and databases. Whilst both systems entail a limitation on rights to privacy and data protection, the risks to a wide range of fundamental rights are higher when it comes to one-to-many processing.

The threats of hacks and other cybersecurity breaches also increase compared to one-to-one systems.

By positing the new processing as “one-to-few” (when in reality, it is still one-to-many biometric *identification*), the Commission is further trying to use language to obfuscate what the proposal puts forward, and to create a false sense of reassurance. This is likely because the process that the DTC will rely on is one known as “closed-set biometric identification”, a type of processing that is sometimes misleadingly referred to by companies as ‘biometric authentication’ in order to try to make it seem less sinister and less risky.

However, the reality is that this proposed Regulation and DTC will establish a series of biometric databases and processing systems, amounting to rights-limiting processing and a normalisation of biometric mass surveillance systems.

The actual nature of this processing is buried in Article 1.1.(c), (“secure transmission of digital travel credentials”). This technocratic language hides the crucial fact that this step includes the establishment of facial image databases which will be used for biometric identification. Furthermore, according to Article 16.1.(a), implementing acts will be used to define factors including “backend services and Traveller Router,” which seems to allude to the new facial image databases.

Given the fact that the proposal does entail new biometric processing, it is clear that the safeguards for the processing of sensitive biometric data, as outlined in Recitals (10), (11) and (12), are nowhere near sufficient. The processing of facial images and other personal data in the DTC system constitutes a limitation to both the right to respect for private life and the right to the protection of personal data.

Limitations must be provided for by law, which must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse.[3] The central storage of facial images is a very concrete risk of abuse which is not addressed in the proposal.

Furthermore, the proposal does not contain any concrete security requirements for the processing of biometric data (facial images) received by Member States, even though this part of the DTC system arguably presents the greatest data protection and cybersecurity risks for passengers due to the storage of their facial images for potentially several days. The EM mentions on page 12 that Member States, on average, will only need to invest EUR 2 million to implement digital travel credentials

[3] C-311/18 Facebook Ireland and Schrems, para. 176

at their external borders. The necessary infrastructure includes facial recognition cameras at all external border crossing points (all lanes with DTC support), as well as a distributed server infrastructure for receiving and securely handling facial images and other DTC data.

It does not seem plausible that these sensitive data can be adequately protected through an infrastructure investment of just EUR 2 million per Member State (on average). The Commission does not seem to have considered the real costs of secure systems. The Impact Assessment (Annex 4) only mentions examples of equipment that was used in Finland and Croatia during limited trials.

4. **Entrenching systems of surveillance, securitisation and discrimination**

Unlike with the new eIDAS Regulation 2024/1183 (Art. 5.a.16(a)), or the 2021 EU digital COVID certificate, there is no provision in the proposed Regulation which would prevent an issuing authority from being able to track every use of the travel app. This would allow governments to build up a detailed picture of everyone's travel habits and border crossings, even if there is no reasonable suspicion to justify this intrusion into people's privacy. This is deeply concerning from the perspective of disproportionate state surveillance, and also creates the possibility that hackers or other malicious actors could also access these data.

In addition to this mass surveillance potential, the proposal fails to build in sufficient safeguards. Whilst the eIDAS Regulation also creates safeguards for the processing of personal data (for example, the ability to conduct transactions pseudonymously (Art. 5), the requirement for open source code and security by design (Art. 5.a)), these are conspicuously absent in the proposed DTC Regulation. Whilst technical safeguards and cybersecurity requirements are noted as important by the EM (p.13), they are not in any of the proposed articles or recitals. The EM also explains that because no new processing is undertaken, there is no need for other safeguards. This is an assertion with which we strongly disagree, particularly in the biometric context which is explored in the previous section.

The risks posed by possible arbitrary state surveillance affect everyone, but particularly and disproportionately impact people on the move, in particular third-country nationals, who are already subject to discretionary and often discriminatory border policies, as well as those in positions which challenge power (such as journalists, political dissidents, human rights defenders). The DTC proposal exists within what the Equinox Racial Justice Initiative reveals to be a broader framework of hostile borders and securitisation policies that construct people on the move as a threat to the European way of life, and we have concerns that the proposal will exacerbate these harms.

Whilst on the surface, the proposed Regulation purports to be about making travel more convenient, the Explanatory Memorandum reveals that profiling 'risky' travellers is an underlying motivation:

> *"border authorities will have more time and resources to focus on risk profiles [...] [including to] prevent irregular migration" (p.4)*
>
> *"allowing also for a better use of resources at local level, allowing them* [border agents] *e.g. to focus on risk analyses, patrolling and other tasks"* (p.12).

Whilst it is packaged in technocratic language, the reference to "risk profiles," "risk analyses … and other tasks" should be read in the context of the wider aim of the Regulation:

> *"by enabling "pre-arrival border checks" and "pre-cleared" passengers, before their arrival at the border-crossing point."* (EM p.12)

The proposal stratifies people into those that are pre-cleared, compared to those that are marked out as suspicious or risky, and therefore subject to increased attention at the physical border. This creates convenience for some, whilst inevitably building in hassle and suspicion against certain groups of people. And there is no right to information or explanation created for those whose pre-arrival checks are unsuccessful.

Additionally, whilst the EM states that external border checks are necessary to prevent "internal border controls" (p.1), we are concerned that there may be a motivation or possibility for the digital travel app and/or digital identity card proposal to facilitate intra-Schengen checks, posing a risk to freedom of movement. The fact sheet accompanying the proposals explains that the proposals "will make traveling to and *within* [italics for emphasis] the Schengen area easier and more secure."

Comments made by the Commissioners at the launch of the proposal make similar allusions. It is not clear how the proposals would relate to inter-Schengen travel, but it is important that the new Regulations do not lead to new internal border checks, nor facilitate arbitrary identity checks of minoritised people within the EU, which are often seen alongside discriminatory policing practices.

5. The coercive effect of ‘convenience’ in digital systems

We are glad that the use of the digital travel app and credentials will be voluntary, creating “travel documents that travellers may use, if they so wish” (EM p.7). This is an important safeguard in the context of the proposed Regulation.

That being said, even though the proposal explains that it will follow rules of consent (Recital (11)), the discussion in the Explanatory Memorandum (p.38) presents a one-dimensional understanding of consent, for example the right to withdraw such consent. This is an important part of consent, but does not by any means present a holistic picture.

What is not taken into account is the coercive impact of such systems. Firstly, this can come from the promotion of such systems as an easy and convenient solution, whilst minimising the potential impacts on privacy and data protection (as seen throughout the IA and EM to the proposal). Following their significant investment in the DTC system, Member States will inevitability promote the use and uptake of the new system.

Secondly, the security context in which such systems are used has an intrinsic coercive effect. Speaking anecdotally as the authors of this submission, several of us have tried to exercise our right not to use e-gates, and have been instructed in no uncertain terms to use them. The imbalance of power between the traveller and the border authority is so profound – and the consequences of seeming ‘suspicious’ or ‘difficult’ so profound in the often discretionary process of immigration – means that the individual has very little power or genuine control. It is therefore inaccurate to posit the system as allowing “active consent” (IA p.13).

This issue is even more profound for people of colour, Muslim people, and other minoritised groups, who are disproportionately constructed as security threats and treated to over-policing and increased interrogation in border and travel situations. In these contexts, people will likely be even less willing to exercise their supposed free choice not to use the DTC or the e-gates, for fear of being harrassed, detained or denied travel.

Thirdly, for those choosing to use alternative systems (e-gates or traditional border agent kiosks) it is foreseeable that Member States will reduce the resources to run these options, and may even make the physical process more cumbersome (e.g. having to take a longer route). Yet the proposal still claims that “[d]ue to the voluntary nature of using digital travel credentials, the principles of non-discrimination and inclusivity are respected” (EM p.14).

It is important to remember that consent must be freely given in order to constitute a valid legal basis for the processing of personal data. Recital 43 of the General Data Protection Regulation (GDPR) clarifies that consent is unlikely to be freely given when there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority, For example, in C-291/12 Schwarz para. 32, the Court of Justice of the EU held that the storage of fingerprints in passports cannot be based on the consent of the data subject because holding a passport is essential for people.

Whilst there is a presumption against consent being a valid legal basis when the controller is a public authority, there are of course exceptions to this general rule. However, the onus is on the Commission and Member States to demonstrate that the traveller (data subject) is genuinely presented with a free choice whether to use the DTC or not.

It is not sufficient that passengers are properly informed that the use of DTC is voluntary without any dark patterns on websites with information about EU border check procedures. If the waiting time before the actual border check (where some 20 seconds is allegedly saved by using DTC) is systematically longer for passengers who do not consent to using DTC, it’s highly questionable that consent to processing of DTCs can be said to be freely given. This applies to EU citizens as well as third-country nationals, even though the two groups of persons are subject to different border checks under the Schengen Border Code.

For these reasons, it is vital that e-gates, and even more critically, traditional border lanes with manual checks, remain genuinely viable alternative options. They must be properly resourced to ensure that those choosing these alternatives are not disadvantaged by this choice. The traditional border lanes will remain the only option for third-country nationals that cannot use DTC, for example because eu-LISA app cannot access their passport chip, the data from the chip cannot be validated by the app, or because they do not have a passport chip.

We also raise concerns about the legal basis under GDPR Article 6(1) and 9(2) for the processing of personal data in the DTC system. The proposal seems to suggest that consent will be legal basis, although this is not very clear since the reference to consent could also mean that the use of DTC is voluntary.

6. Technical, political and economic motives for digitalising travel documents

Whilst the package is presented as the “digitalisation of passports and ID cards” to the public, the proposal is really about digital pre-submission of information (digital travel credentials) from the chip of existing physical passports and ID cards to border authorities. Travellers will still need to carry the physical document, in part for security reasons. This means that there will be no benefit for people who have lost their passport or who temporarily cannot access it (for example because it has been submitted as part of a visa application process).

As described in the IA and supporting material, in order to use the DTC, people will need to install an eu-LISA app on their smartphone, scan their passport chip, and then subject themselves to facial recognition with a liveness check, where an AI system will instruct them to e.g. move their head in certain ways until the AI system is “satisfied” than the smartphone camera is capturing a real person and not a deepfake image fed into the camera.

In the Impact Assessment, this process is estimated to take 2-3 minutes, but there will be cases that take considerably longer or where the process cannot be completed, e.g. because the passport chip cannot be validated or because the facial recognition test fails. Unlike the current e-gates at border crossing points, the lighting conditions in a person’s living room are not optimised for facial recognition. Moreover, the inherent racial and gender biases of facial recognition technology will inevitably lead to bad user experiences for some communities. Whilst facial recognition providers frequently claim high accuracy rates for their technology, failures and false alerts still disproportionately affect racialised people. And even a very high accuracy rate can amount to a lot of errors when there are hundreds of millions of border crossings each year.

Some passengers will want to engage in this process (digital pre-submission of travel credentials) and will perceive and/or experience enhanced convenience due to the process ‘going digital’. However, many other travellers, whether EU citizens or third-country nationals. will more pragmatically consider the benefits and costs (time and trouble) of using DTC versus the traditional border procedures. As already discussed, the Commission estimates that the border check (inspection and check of the passport and database checks) can be done about 20 seconds faster with the DTC. For the individual traveller, it does not make a lot of sense to use a couple of minutes to scan their faces with an app, including a potentially cumbersome liveness test, and submit their sensitive biometric data to a central server, via an eu-LISA router, with all the data protection and privacy risks that that entails, in order to save just 20 seconds during the border check procedure.

Union citizens and other persons with the right to free movement do not have to submit any information to border authorities in advance. For third-country nationals, the DTC will mean an additional pre-submission of information for each journey to and from the EU on top of obtaining a visa or ETIAS travel authoritsation (both of which are not necessarily tied to a specific journey to the EU).

The traditional border lanes, with either manual checks or e-gates (where the passport chip is read by the e-gate), will still be needed. First of all because it will be voluntary for travellers to use DTC. Secondly, it must also be borne in mind that some third-country nationals will not be able to use DTC even if they want to. Not all countries issue passports with a chip conforming to ICAO standards, not all countries allow the chip to be read by their passport holders or a smartphone app, and the data on the chip cannot always be properly validated because the necessary certificates are not available to the eu-LISA app. In the Impact Assessment, the Commission has not made any attempt to assess how many third-country nationals travelling to the EU will be able to use the eu-LISA app (if they want to). The Impact Assessment (p. 29) only notes that some EU Member States have prohibited access to the passport chip. This limitation can be remedied by EU law, but the EU cannot unilaterally impose requirements on passports issued by non-EU countries.

When using the DTC, travellers will be entering and leaving the EU through dedicated border lanes equipped with facial recognition. This involves calculating a biometric template from the travellers' faces and comparing this template to the database of persons that are expected to pass through the the border-crossing point on that day and time (1:N comparisons). This processing of sensitive personal data is only lawful if one of the exceptions in GDPR Article 9(2) applies, in this case consent of the data subject (point a). However, consent has only been obtained from persons using DTC, which means that border lanes with facial recognition must be physically separated from other border lanes with manual checks, so that non-DTC passengers are not subjected to the processing of a biometric template.[4]

The necessity of maintaining existing border-check procedures and keeping them physically separated from border lanes using DTC (as required by the GDPR) invariably means additional expenditure for Member States. Moreover, if the uptake of using DTC is uncertain and may change over time when the initial excitement of "digital" passports wears off, capacity planning at border-crossing points may become even more difficult (and expensive) for Member States. This problem does

[4] See EDPB Guidelines 3/2019 on processing of personal data through video devices, paragraph 78 ("The check points with facial recognition need to be clearly separated, e. g. the system must be installed within a gantry so that the biometric templates of non-consenting person will not be captured. Only the passengers, who will have previously given their consent and proceeded with their enrolment, will use the gantry equipped with the biometric system.")

not seem to be considered by the Impact Assessment, which simply assumes that Member States can fairly easily integrate DTC into their existing border procedures.

Besides the political agenda of digitalising as much as possible, the motivation for the proposal is making border procedures more efficient (as criticised earlier in this submission). Several challenges faced by current border procedures are highlighted in the EM and IA, including the large number of checks against EU and national databases that have been added to Article 8 of the Schengen Border Code. When travellers submit their DTC in advance, these checks can be performed before the traveller reaches the border-crossing point. The EM page 3 also mentions that required verification of the authentication and integrity of the passport chip must sometimes be skipped by border guards due to travel peaks and technical malfunctions. One of the current problems is that the inspection device may not have access to the certificated needed to validate the chip (Impact Assessment, p.17).

The validation of the chip will instead be performed by the eu-LISA app, which of course take some pressure off equipment capacity at the border-crossing point, but it is not explained how the technical malfunction issues will be addressed. The eu-LISA app can also suffer from technical failure, where the consequences will be a lot greater (single point of failure) than technical failure at a single border-crossing point.

We have no reason to doubt that these problems exist, and that the political narrative of protecting Europe’s borders against terrorism and migration has led to unforeseen burdens for travellers as well as authorities, but there must be other ways of addressing them than pre-submission of DTC. This could include hiring more border guards, upgrading database capacity at the Union and Member States level to allow more database lookups per minute (ensure capacity for peak periods), and acquiring more equipment to validate the passport chip. If the certificates required for this validation can be made available to the centralised eu-LISA app, it must also be possible to make the certificates available for equipment at Member States’ border-crossing points.

The Commission does not appear to have considered these alternative options for making border crossing at the EU external borders more efficient. All policy options considered involve the DTC, making it a foregone conclusion.

Last, but not least, we find it almost ironic that the role of fingerprints stored in the passport or ID card chip are downplayed by the new proposal. For technical reasons, it is not possible to read fingerprints from the chip and use them for DTC. As is well known, the storage of fingerprints on the chip has been subject to considerable public opposition and even litigation before the CJEU (two cases).

Despite the secrecy of Member States regarding access to fingerprints, there are strong indications that the fingerprint data is rarely accessed on the chip because of Member States' reluctance to share the certificates required for accessing this part of the chip with each other. If the DTC is the future of digital travel, as the Commission seems to believe, fingerprints will be accessed even more rarely than today.

This calls into question the proportionality of requiring storage of fingerprints on the chip in the first place, although this question, strictly speaking, is outside the scope of the DTC proposal. However, it is relevant for the ongoing deliberations by Council on the revised proposal on EU identity cards [COM(2024) 316 final] following the annulment of Regulation (EU) 2019/1157 by the CJEU in the judgment C-61/22.

7. Scope creep and environmental questions about the Digital Travel Credential

As repeatedly emphasised by then-Commissioner for Justice, Didier Reynders, at the press conference launching the package, one of the main aims of the package is to increase competitiveness and innovation for businesses in Europe. There is a clear motivation for the DTC and/or digital identity to be used by businesses in a variety of services creeping far beyond travel:

> "*It could increase efficiency for carriers on a voluntary basis, as they could integrate digital travel credentials into their current workflows. It also enables further use cases of digital travel credentials by EU citizens, by establishing an electronic attribute for the EU digital identity wallet that can be used for e.g. proving one's identity within the EU or even abroad, if accepted by third countries*." (EM p.12)

Whilst the main purpose of the proposal is to create a DTC to facilitate EU external border crossing, it can be stored in the European Digital Identity Wallet (Article 4.2). The Explanatory Memorandum explains that the DTC can be uploaded to a person's European Digital Identity Wallet:

> "*Digital travel credentials could be stored alongside digital driving licences, medical prescriptions and other documents in the EU digital identity wallet, constituting an electronic attestation that can be used for purposes that go beyond travel, e.g. as a digital identity document for both remote and in-person transactions*." (EM p.6)

It is not explained in the proposal just how European competitiveness will be enhanced by the package, but without proper guardrails or rights protections, we are concerned at the implication that the DTC could enter into many parts of our lives, possibly underpinned by private financial motivations. There is a vast industry who for years have been lobbying the EU to try to make their ‘seamless’ travel ‘innovations’ the EU norm, due to how profitable the uptake of these technologies can be.

At the same time as pushing this industry-led ‘seamless’ travel agenda, the proposal does not engage with possible environmental issues arising from digitalisation. The processing, analysis and storage of data rely on extractive technologies and resource-hungry data centers. The cost to people and planet of these systems is not reckoned with by the package, but should be a concern for the aim of mass uptake of the DTC.

Moreover, the core impulse of the DTC is to enable even higher volumes of travel, which is in itself problematic. With air travel a key contributor to the climate emergency, it is concerning that EU laws would promote an uptick in something so harmful to the environment.

From the creation of mass facial image databases, to the over-policing of people on the move, to the lack of technical or legal safeguards, the DTC as proposed by the Commission would not be fit for purpose for border crossings, let alone to become a part of our daily lives.