One ID
FAQs on PRIVACY

How One ID will Protect Passengers' Personal Data

Frequently Asked Questions

Purpose

The introduction of biometrics fundamentally changes the type of passenger personal data that is collected and shared within the air travel journey. Because the One ID concept deals with such data, privacy and data protection concerns are often raised.

The industry and governments are working together to understand detailed privacy implications and seek adequate clarifications to ensure any One ID project can be applied, across jurisdictions, allowing the industry to use passengers' biometric recognition for identity verification throughout the travel process while making sure to respect and protect passengers' privacy and protection of their data.

This document aims to answer these concerns for all actors in the travel data process and demonstrate the significant focus that One ID has on data privacy and protection. It is the vision of the IATA that collaborative projects to implement One ID processes do so with a clear commitment to set and enforce high standards of privacy so that passengers' personal information is protected to a greater standard than current processes.

How will passenger data be used?

One ID relies on secure and lawful sharing of data amongst stakeholders. One ID supports the principle that data should be processed transparently, lawfully and fairly.

Following the principle of data minimization, only strictly necessary personal data shall be collected and only for the express purpose for which it is collected; passengers shall be properly informed and where stakeholders wish to use data for additional purposes, they should define those purposes and seek the appropriate legal grounds and passenger consent.

Importantly, the quality, accuracy, integrity and overall security standards of the personal data should be set high to protect the privacy of the passenger.

It is important to note that much of the personal information exchanged currently in international air travel from air carriers to governments is mandatory, such as Advance Passenger Information (API) under the Chicago Convention, Annex 9, and the United Nations Security Council resolutions 2178 (2014) and 2396 (2017). While One ID will not remove the requirement for the exchange of this data, it could provide opportunities to minimize the amount of personal data managed by industry while facilitating this exchange.

How is the data shared between stakeholders?

As the One ID standards for interoperability and data exchange are yet to be determined, this question can not be answered in full at this time.

However, as Privacy by Design and Default are key principles of One ID, any solution determined will set high standards of privacy and, security ensuring personal data is protected to a greater level than legacy processes.

What data is collected under One ID?

In order to understand what data will be collected in One ID, we need to understand what data is collected and shared now and for what purpose.

One ID considers there to be three types of data:

1. Data necessary to provide core travel services (i.e. getting the passenger to and from their destination);

2. Additional process data such as touchpoints passed, time stamps, records of exemptions, any red flags and signals (which can help deliver an optimal service to passengers); and

3. Data for other services (nonessential elements for such as commercial or marketing purposes.).

Consent for the latter should not be bundled with the first two and importantly passengers should be able to opt in and out of all nonessential services without this affecting the provision of core services.

Airlines, airports and governments need to determine what the minimum necessary data requirement is to facilitate the traveler journey in a seamless manner using only a biometric identifier to pass through controlled checkpoints.

There is currently passenger data collected and exchanged for the purposes of travel. The Chicago Convention on International Civil Aviation Annex 9 – Facilitation principle 1.2 API requires traveler data to be sent in advance of arrival at their physical destination. The data is used to pre-screen travelers before they land and to help states to effectively manage threats and facilitate processing.

One ID envisages a passenger data set that contains all the necessary digital identity information, including biometrics of the passenger, flight information (similarly to current API flight information) and travel authorizations. It may include additional process information (e.g. record of the passenger's transaction through a touchpoint).

Access controls need to be in place in order to determine the privacy and security of the data: only the authorized party can access the necessary data required to facilitate a check point in the travel flow. Wherever possible, pseudonymization[1] shall be implemented to protect the identity of the individual.

The passenger shall have clear visibility on which personal data is used and how and be able to opt in/out for non-core functions such as commercial transactions, customer surveys or direct marketing.

Why does privacy and data protection legislations matter?

In Europe, the General Data Protection Regulation (GDPR) Came into force on the 25th May 2018 .

GDPR requires organizations to ensure that privacy and data protection is a key consideration in any processing of personal data. The GDPR has an extra-territorial scope and also applies to companies based outside of the EU targeting (sales of goods or services, monitoring of behavior) individuals located in the EU.

Although GDPR is currently considered as the privacy gold standard, the focus of the legal analysis for One ID processes shall not be limited to GDPR only. Privacy Regulations in all territories must be considered. Brazil, China, Thailand and Russia are currently reviewing privacy legislations or have just enacted new legislation. We strongly encourage the different stakeholders to monitor their developments and ensure compliance.

What is Privacy by Design?

Privacy by design is one of the key principles of One ID.

Quoting the privacy Regulator in the UK, privacy by design means integrating or 'baking in' data protection into your processing activities and business practices, from the design stage right through the lifecycle.

Data controllers [2]must put technical and organizational measures such as pseudonymization in place – to minimize personal data processing.

It is not a new concept, but it is now a legal requirement under the GDPR.

What is Privacy by Default?

Privacy by default is one of the key principles of One ID.

Data protection by default requires you to ensure that you only process the data that is necessary to achieve your specific purpose.
The purpose for collecting the data needs to be specified before the processing starts and individuals appropriately informed. The data can only be used for the purpose identified.

The article in this link provides further reading on the concepts of Privacy by design and by default.

[1] Pseudonymization is a de-identification process by which personally identifiable data fields are replaced by one or more artificial identifiers, or pseudonyms

[2] Data controller as defined by the EU in this link

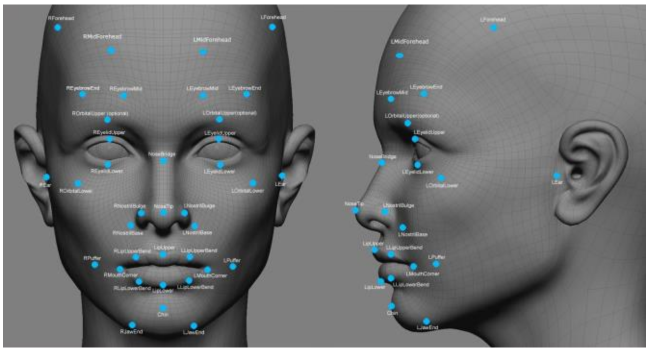
What is the difference between biographical data, a biometric and a biometric template?

In the context of One ID **biographical data** is the personalized information that appears on a passenger's passport as text or can be read in a machine-readable zone. As such it includes data elements like name, nationality, sex, date and place of birth.

A **biometric** on the other hand, is a "measurable, unique, physical characteristic or personal behavioral trait"[3] that can be used to verify an individual's identity.

In the context of One ID, this means face, finger or iris, inline with the biometrics currently prescribed in ICAO standards.

Legislation in many countries considers biometric data as a special/ sensitive/important category of personal information, subject to specific requirements that the stakeholders will have to consider.



A **biometric template** is a machine-encoded representation of a biometric trait created by a computer software algorithm'[4]. This template can then be compared against other collected templates, to help confirm whether the templates are from the same person.

From a privacy perspective, biometric templates offer additional protection, as even if someone gains access to the data, it is very difficult to reconstruct the original image.

Biographical data and biometric data should be kept separate in order to reduce privacy and security risks.

[3] ICAO Doc 9303, Machine Readable Travel Documents, Seventh Edition, 2015, *Part 1: Introduction.*

[4] ICAO Doc 9303, Machine Readable Travel Documents, Seventh Edition, 2015, *Part 9: Deployment of Biometric Identification and Electronic Storage of Data in MRTDs.*

Does the passenger have to consent?

Consent[5] is a principle of the One ID concept. This means that the passenger should be actively informed that their data is being collected, for what purpose, and provide their consent where necessary according to local regulations.

While there are some aspects of international travel where government border authorities require mandatory information, collected either by the airline in advance of travel or on arrival at the destination, the passenger always has the choice to participate in a One ID process.

Specific consent is required for personal data processing and it may be withdrawn at any time. The recommended practice for One ID projects is to ensure that when undertaking the enrolment of the passenger that the consent is clear, informed and meaningful. Consent should be:

- unbundled from other terms and conditions;
- opt-in, as opposed to a pre-checked box;
- granular, with specific and separate consent for different types of processing; and reversible so that people can withdraw.

Whilst the specifics may vary state by state, it is expected that for most One ID projects, passenger consent will be a critical element. How exactly consent is obtained may differ from project to project and depending on the local and regional requirements, including those of the destination or transited States. It may be persistent (for multiple journeys), or required each time a passenger travels.

The long-term vision would see passengers in control of their own data and trusted digital identity and be able to share their biometric and trip details as they choose with a wider group of service provides to help facilitate and streamline their journey.

Will there be an alternative non-biometric process?

There will need to be alternative process for those who can't, or do not wish to, participate in such a system. This is already the case with many self-service travel options provided by airports, airlines and governments today.

While One ID can significantly improve the passenger experience, those opting out will still be able to complete their journey via traditional manual processing, sharing their documents at each touch point, and their API data will be collected and shared as per current practices.

What happens to the passenger data after the trip is complete?

The recommended practice is that all personal, identifying data is deleted by the industry stakeholder after the data has fulfilled its purpose. This may vary between jurisdictions or where there is a clear legal need and authorisation to retain the data or

[5] Consent is the method adopted but as use cases develop adoption of other methods will be reviewed to ensure the best approach to support security and privacy is preferred.

where the passenger has opted to have that data retained, such as within a frequent flier program membership.

One ID recommends end to end security with data lifecycle protection. This means high levels of responsibility for the security of personal information throughout its entire lifecycle, such as secure methods of destruction, appropriate encryption, and strong access control and logging methods.

What is data transparency?

One ID recommends data transparency.

Data transparency requires organizations to provide clear information about their privacy policies and data processing which must be made available publicly. In addition to this, passengers should have access to clear information on the organization's policies for redress and complaint.

It is important to note here, that while airlines are recommended to inform passengers of the data they are required to send to governments, they are not able to inform passengers what the receiving government uses that data for.

Will biometric and personal data be safe and secure?

One ID relies on a trusted, digital identity and a collaborative Identity Management Platform (IMP) to facilitate the process and exchange of necessary data. This will involve security and protection mechanisms such as cryptography, pseudonymization, anonymisation and data minimization, and policies regarding the data necessary for each specific purpose.

Several government agencies within the aviation sector already collect and use biometrics and biographic passenger information for processing purposes. In addition, other stakeholders such as airlines, handle biographic passenger data and travel details for millions of travelers daily.

Because of this, Advanced technologies and processes already exist to help protection passenger data such as:

- **Secure encryption techniques and protocols** used for transmission and storage of personally identifiable information.
- **Secure storage** which is compliant with local, national and international data storage requirements for personally identifiable information.
- **Defined retention periods and appropriate destruction mechanisms**, to limit the vulnerability and minimize the impact of any breach.
- **Audit and compliance regimes:** to test the systems and ensure that protocols are complied with.
- **Use of biometric templates:** the original biometric is not stored, but rather it is converted into a template (string of multiple numbers) via a one-way process. Each time a new biometric is captured it too is converted into a template, and these unique templates are then compared against each other to confirm an ID. Because the original image is not stored, it means that even if someone gains access to the data, reconstructing the original image is extremely difficult.

How can the passenger trust airlines, airports, and governments to respect privacy regulations?

Airlines, Airports, and Governments developing a collaborative One ID process are encouraged to undertake a Privacy Impact Assessment (PIA) as part of their project to determine upfront whether such a process can be executed within the relevant legal boundaries. The PIA also helps to identify risks in the development to ensure privacy is maintained and protected. The PIA can be made available to help others understand the rationale behind the privacy decisions made, considering the context, nature and purposes of the data processing.

What is a Privacy Impact Assessment (PIA)?

Like projects in other sectors dealing with sensitive data, carrying out a Privacy Impact Assessment is considered best practice for all One ID related projects.

For many stakeholders the PIA will be a mandatory legal requirement. A PIA provides the opportunity for the stakeholders to address privacy concerns that may arise as a result of their specific role in the project and identify mitigation strategies.

PIAs for such projects will generally be reviewed by local privacy and data protection regulators, who may request further information or additional mitigation measures to be put in place if deemed necessary.

This provides an additional level of assurance that privacy has been considered as part of the project design and that passenger rights and data security requirements will be complied with.

What are Operational or Trust Frameworks and how do they relate to privacy?

An operational framework (often referred to as a trust or liability framework) is a set of specifications, rules, and agreements that govern a multi-party collaboration.

In the case of One ID, an operational framework governs identity management within an aviation ecosystem. In addition to roles, rights and responsibilities and technical requirements more generally, it will set out how data privacy will be managed between participating stakeholders.

In a practical sense, it will address who can access what data, when, and for what purpose. It will also set out processes and technical solutions to address data protection, retention and storage, and include details of relevant audit and compliance regimes.

This operational framework will operate alongside any local, national or international privacy requirements to help assure the protection of passenger data.
The objective of the One ID project is to allow for the necessary tools to be in place (appropriate standards and recommended practices as examples) to allow interoperability amongst different frameworks, regardless different cultural, legal, etc. context.

What is One ID doing to ensure privacy for passenger data?

Data privacy is a key cornerstone of the One ID vision.

A Key Contributors Expert working group has been formed, including legal and/or data privacy practitioner/professionals from across the industry to consider and address the documentation and guidance needs for the industry as it considers new pilots and trials of the One ID concept.

A Privacy Key Talking Points document has been specifically written on this subject to go through certain elements of One ID that raise questions with regards to the respect of privacy regulations and framework, such as the type of data being exchanged, what changes from today, the differences in between biographic, biometric or template data, what is required from the passenger standpoints, security of data, etc.

This Privacy Key Talking Points document is a 'living document' and will be regularly updated. It is available on the PEMG Extranet Site.