# KTDI Pilot – Data Protection Impact Assessment (NLD)

# DPIA Introduction

- "A Data Protection Impact Assessment (DPIA) is required under the GDPR any time you begin a new project that is likely to involve 'a high risk' to other people's personal information."
    - Source: gdpr.eu

- This DPIA is based on the template as provided by the Dutch government.

# DPIA - Introduction (cont'd)

- Territorial scope (GDPR, art. 3):
    - The processing of personal data within the Netherlands is in scope of this DPIA.
        - Disregarding whether the Data Subject is a Canadian or Dutch citizen.
    - The processing of personal data within Canada is not in scope of this DPIA.
        - Disregarding the fact that personal data of Dutch citizens may be processed in Canada.

# DPIA Introduction (cont'd)

- Definitions (GDPR, art. 4):
  - Data Subject: an identified or identifiable natural person.
    - Within the context of the KTDI Pilot: a Canadian or Dutch Traveller who makes use of one or more KTDI Services within the territorial scope of the GDPR.
  - Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
    - Within the context of the KTDI Pilot and as far as within the territorial scope of the GDPR:
      - Air Canada.
      - KLM.
      - National Office for Identity Data (NOID).
      - National Coordinator for Security and Counterterrorism (NCSC).
      - Royal Marechaussee (KMar).
  - Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
    - Within the context of the KTDI Pilot:
      - Amsterdam Airport Schiphol (AAS; on behalf of KLM and Royal Marechaussee).
      - Accenture (on behalf of KLM, [redacted] NOID, CBSA, Air Canada).
      - Idemia (on behalf of NOID).
      - VisionBox (sub-processor on behalf of Amsterdam Airport Schiphol).

# DPIA Introduction (cont'd)

- Definitions: in this DPIA the following terms will be used:
  - KTDI Service:

  - Service Provider: a Canadian or Dutch private or public organization which offers a KTDI Service to Travellers.
    - Air Canada;
    - KLM;
    - KMar;
    - NCSC
    - NOID; and
    - Schiphol Airport.
    - Also: Controller.

  - Traveller: a Holder of a Canadian or Dutch e-passport who is eligible to make use of KTDI Services.
    - Also: Data Subject.

(More definitions may be added during the DPIA process.)

# DPIA Scope

# DPIA Scope: KTDI Pilot Process - Departure NLD


In scope of DPIA KTDI.

Out of Scope of DPIA KTDI.
In scope of DPIA Seamless Flow.

Completely in scope of this DPIA.

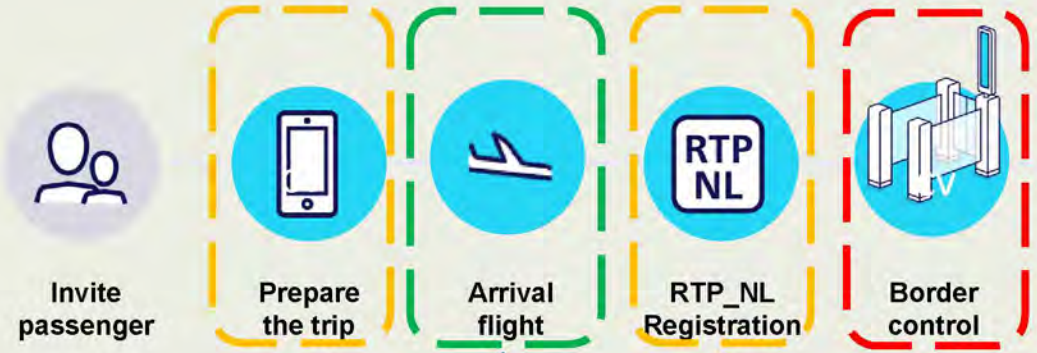
Partially in scope of this DPIA.

Not in scope of this DPIA.

See: 'KTDI NLD Operational Concept Description' for a detailed description of each process step.

In scope of pilot process  Out of scope of pilot process

# DPIA Scope - KTDI Pilot Process – Arrival NLD




Out of scope of DPIA KTDI.
In scope of DPIA Seamless Flow.

In scope of DPIA KTDI: applying using the KTDI App.
Out of scope of DPIA KTDI but in scope of DPIA RTP-NL: processing the application.

In of scope of DPIA KTDI: data processing in the Netherlands (territorial scope GDPR).

In scope of DPIA KTDI.

In scope of pilot process  Out of scope of pilot process

# A.
# Characteristics of Data Processing

# Characteristics of Data Processing

Describe the proposed data processing, the goals of the data processing and the importance of the data processing to the stake holders:

- Global overview of the relevant processes.
  - See slides xx and xx.
    - Also see document 'KTDI NLD Operational Concept Description' for a detailed description of each process step.
  - See slides xx to xx for a high-level description of the evolution of relevant processes from manual processing up to KTDI enabled processes.
  - See slides xx to xx for an overview of the technological support of the processes.

- Personal data which are processed → see slides xx to xx.
  - Also see document 'KTDI Pilot - data processing (appendix to DPIA)'.

- Data flows.
  - See document 'KTDI pilot – NLD Data Flows'.

# A.1 Characteristics of Data Processing

*Processes*

# Characteristics of Data Processing (cont'd)

- The KTDI concept is a new way of enabling the execution of existing business processes of Service Providers.
- Some KTDI specific processes will be introduced.

| Process | New/existing process | If existing process is adapted to KTDI: what is different? |
|---|---|---|
| Invite Traveller | [redacted] specific process. | -- |
| Create KTDI Profile | [redacted] specific process. | -- |
| Create Digital ID | [redacted] specific process. | -- |
| Check-in | Existing process. | • After check-in: Boarding Pass will be sent to Travellers' [redacted] Wallet. |
| Prepare the Trip | [redacted] specific process. | -- |
| Priority Access Security | Existing process. | • Traveller requests to make use of this KTDI-adapted process in advance<br>• Biometric recognition of Traveller. |
| Border Control | Existing process. | • Traveller requests to make use of this KTDI-adapted process in advance<br>• Biometric recognition of Traveller. |
| Boarding Access | Existing process. | • Traveller requests to make use of this KTDI-adapted process in advance<br>• Biometric recognition of Traveller. |

# Characteristics of Data Processing – cont'd

Global overview of the relevant processes.

- First time Dutch Traveller; flight NLD→CAN.


- Second time Dutch Traveller; flight NLD→CAN.


In scope Out of scope

# Characteristics of Data Processing – cont'd

Global overview of the relevant processes.

- First time CAN Traveller; flight CAN→NLD.


- Second time or more CAN Traveller; flight CAN→NLD.
- Dutch Traveller; flight CAN→NLD.

# Characteristics of Data Processing

Global overview of the (technological) development of KTDI related processes – border control

- Manual checks: since a long time the Royal Marechaussee (KMar) manually checks travellers and their travel documents upon arrival and departure at Schiphol airport. This includes a visual inspection of the travel document as well as a check whether the traveller who presents the travel document is the rightful holder of it (by comparing the face of the traveller with the photo in the Visual Inspection Zone of the passport.)
    - From 2012 to 2015, authenticity of passports wasd a manual process; checks of the enforcement databases were semi-automatic (manual input of relevant data; automated search for hits).
    - Since 2015, authenticity checks of the passports and the checks of the enforcement databases are fully automated.

- In 2014, Self-Service Passport Control is introduced at Schiphol Airport. The traveller presents their e-passport to a scanner in an e-gate, which scans the holder page (including the optical MRZ) as well as the digital MRZ (RFID chip, Data Group 1). The digitalized data of the optical/digital MRZ is used to check enforcement databases. A live facial image of the traveller is taken and compared to the photo stored in the RFID chip (Data Group 2) in order to determine whether the traveller in the e-gate is the rightful holder of the e-passport.
    - These checks are fully automated.
    - In case of hits/errors or other unclear situations, a border guard will intervene/assist the traveller.

- KTDI is a next step in which a traveller shares rheir personal data with the KMar before he arrives at a border crossing point. This can be done off-airport at a time and location that suits the traveller. KTDI enables the KMar to process the personal data in advance, which pertain to the concept of information-based acting (goede vertaling van informatiegebaseerd optreden?).

# A.2
# Characteristics of Data Processing

## *Data*

# Characteristics of Data Processing (cont'd)

Personal data which are processed - enrollment.

| Data element* | Special Category of Personal data?** | Data Subject*** | Source | Recipient*** | Controller*** | Processor*** |
|---|---|---|---|---|---|---|
| Given Names | No | Traveller | Holderpage, RFID Chip DG1 | NOID | NOID | |
| Surnamer (including prefix) | No | Traveller | Holderpage, RFID Chip DG1 | NOID | NOID | |
| Date of Birth | No | Traveller | Holderpage, RFID Chip DG1 | NOID | NOID | |
| Place of Birth | Sensitive data | Traveller | Holderpage | NOID | NOID | |
| Personal Number | National Identification Number | Traveller | Holderpage, RFID Chip DG1 | NOID | NOID | |
| Identification Feature (portrait of the holder) | Sensitive data - biometric data | Traveller | Holderpage, RFID Chip DG2 | NOID | NOID | |
| Sex | No | Traveller | Holderpage, RFID Chip DG1 | NOID | NOID | |
| Live Facial Image | Sensitive data - biometric data | Traveller | Traveller | NOID | NOID | |
| Nationality | Sensitive data | Traveller | Holderpage, RFID Chip DG1 | NOID | NOID | |
| Passport Number | Sensitive data | Traveller | Holderpage, RFID Chip DG1 | NOID | NOID | |
| Document Code | No | Traveller | Holderpage, RFID Chip DG1 | NOID | NOID | |
| Date of Issue | No | Traveller | Holderpage | NOID | NOID | |
| Date of Expiry | No | Traveller | Holderpage, RFID Chip DG1 | NOID | NOID | |
| Issuing State or Organization | Sensitive data | Traveller | Holderpage, RFID Chip DG1 | NOID | NOID | |
| Flagged in national stolen/lost travel document database | Sensitive data | Traveller | Verificatieregister | NOID | NOID | |

# Characteristics of Data Processing (cont'd)

Personal data which are processed – check-in.

| Data element* | Special Category of Personal Data? ** | Data Subject*** | Source | Recipient*** | Controller*** | Processor*** |
|---|---|---|---|---|---|---|
| | | | | | | |
| Airport of Departure | No | Traveller | Airline | Airline | Airline | |
| Flight Number | No | Traveller | Airline | Airline | Airline | |
| Date of Departure | No | Traveller | Airline | Airline | Airline | |
| Passenger Sequence Number | Sensitive data | Traveller | Airline | Airline | Airline | |

# Characteristics of Data Processing (cont'd)

Personal data which are processed – border control.

| Data element* | Special Category of Personal Data? ** | Data Subject*** | Source | Recipient** * | Controller** * | Processor** * | Data necessary for executing Border Control Process | Data necesary for background check | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | SIS2 | E&S | SLTD |
| Given Names | No | Traveller | Holderpage, RFID Chip DG1 | n.a. | MoD | Schiphol | Yes | Yes | Yes | No |
| Surname (including prefix) | No | Traveller | Holderpage, RFID Chip DG1 | n.a. | MoD | Schiphol | Yes | Yes | Yes | No |
| Date of Birth | No | Traveller | Holderpage, RFID Chip DG1 | n.a. | MoD | Schiphol | Yes | Yes | Yes | No |
| Identification Feature (portrait of the holder) | Sensitive data - biometric data | Traveller | Holderpage, RFID Chip DG2 | n.a. | MoD | Schiphol | Yes | Nee | Nee | No |
| Sex | No | Traveller | Holderpage, RFID Chip DG1 | n.a. | MoD | Schiphol | Yes | Yes | Yes | No |
| Live Facial Image | Sensitive data - biometric data | Traveller | Holderpage, RFID Chip DG1 | n.a. | MoD | Schiphol | Yes | Nee | Nee | No |
| Nationality | Sensitive data | Traveller | Holderpage, RFID Chip DG1 | n.a. | MoD | Schiphol | Yes | Yes | Yes | No? |
| Passport Number | Sensitive data | Traveller | Holderpage, RFID Chip DG1 | n.a. | MoD | Schiphol | Yes | Yes? | No? | Yes |
| Document Code | No | Traveller | Holderpage, RFID Chip DG1 | n.a. | MoD | Schiphol | Yes | Yes? | No? | Yes? |
| Date of Expiry | No | Traveller | Holderpage, RFID Chip DG1 | n.a. | MoD | Schiphol | Yes | Yes? | No? | ? |
| Issuing State or Organization | Sensitive data | Traveller | Holderpage, RFID Chip DG1 | n.a. | MoD | Schiphol | Yes | Yes | No? | Yes? |
| Video Footage (CCTV) | Sensitive data - biometric data | Traveller | CCTV | n.a. | MoD | Schiphol | Yes | No | No | No |
| Flagged in Law Enforcement Database | Personal data relating to criminal convictions and offences (only in case of 'hit') | Reiziger | SISII, E&S, SLTD | n.a. | MoD | Schiphol | Yes | No | No | No |
| HitNoHitCode | Personal data relating to criminal convictions and offences (only in case of 'hit') | Reiziger | SISII, E&S, SLTD | n.a. | MoD | Schiphol | Yes | No | No | No |
| Match on Data Element | Personal data relating to criminal convictions and offences (only in case of 'hit') | Reiziger | SISII, E&S, SLTD | n.a. | MoD | Schiphol | Yes | No | No | No |
| Required Action | Personal data relating to criminal convictions and offences (only in case of 'hit') | Reiziger | SISII, E&S, SLTD | n.a. | MoD | Schiphol | Yes | No | No | No |
| Gevarenklasse | Personal data relating to criminal convictions and offences (only in case of 'hit') | Reiziger | SISII, E&S, SLTD | n.a. | MoD | Schiphol | Yes | No | No | No |
| Description | Personal data relating to criminal convictions and offences (only in case of 'hit') | Reiziger | SISII, E&S, SLTD | n.a. | MoD | Schiphol | Yes | No | No | No |

# Characteristics of Data Processing (cont'd)

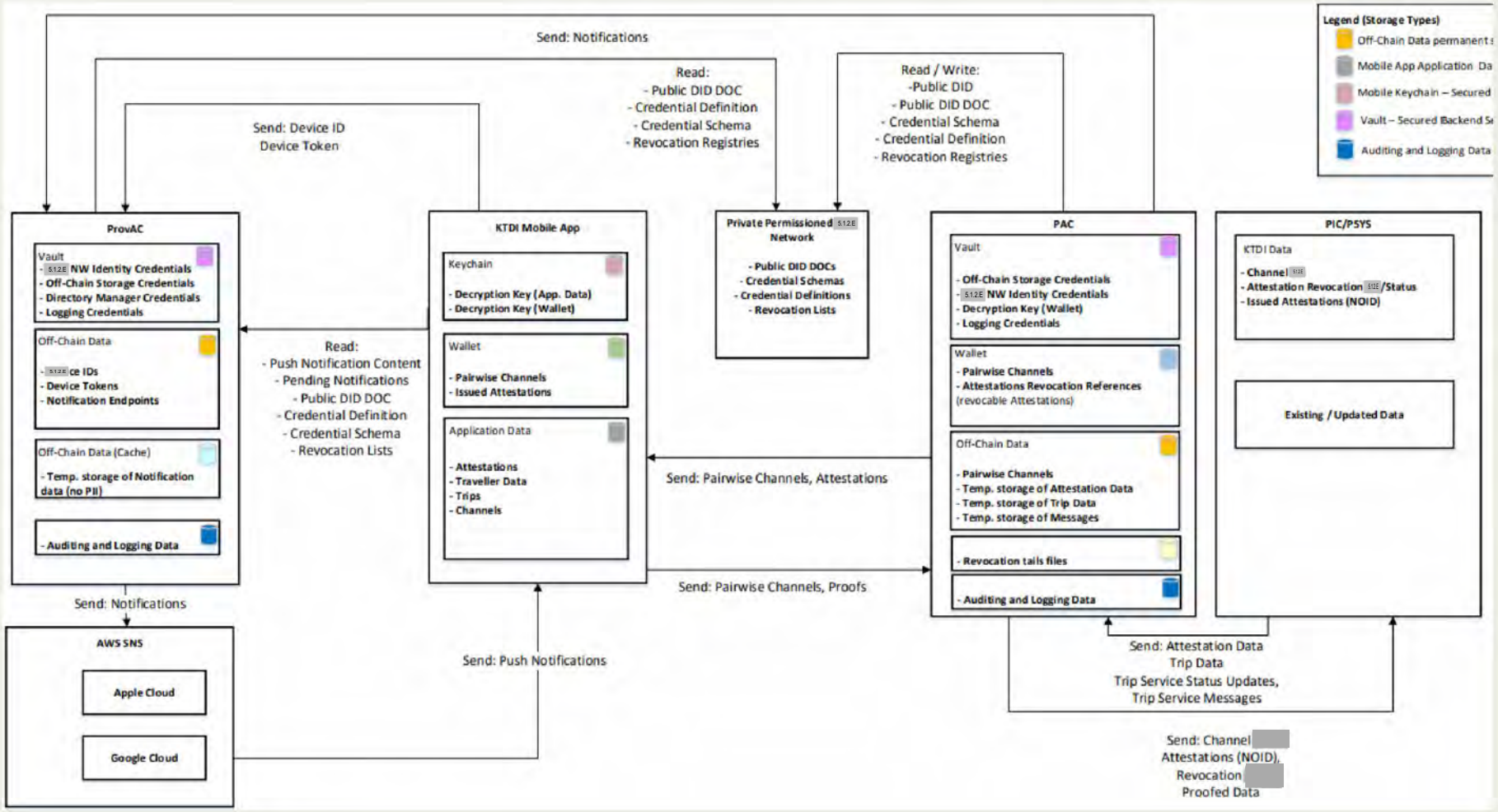
Personal data which are processed – boarding.

| Data element* | Special Category of Personal Data? ** | Data Subject*** | Source | Recipient*** | Controller*** | Processor*** |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |

- TBD

# Characteristics of Data Processing (cont'd)

KTDI Pilot – 'Data Architecture'.



# A.3 Characteristics of Data Processing

## *Goal of Data Procesing*

# Characteristics of Data Processing (cont'd)

- Goal(s) of the data processing.
    - The main goal of the data processing is to enable a seamless travellers journey where the Traveller (the Data Subject) will be identified using biometrics. This will be possible because the Traveller requests to make use of specific KTDI Services by sending the required data to the Service Provider. While at the airport, the Traveller will not need to show their Travel Document* or Boarding Pass at selected touch points since they wil be recognized using biometrics.

    - Another goal of the data processing is to enable the Service Providers to process service requests of Travellers even before the Traveller's journey has begun, thereby expediting their processes at the airport.

*) Due to the Schengen Borders Code, Canadian Travellers do need to collect and entry/exit stamp at the Dutch Border upon arrival/departure.

# A.4
# Characteristics of Data Processing

## *Controllers, Processors & Locations*

# Characteristics of Data Processing (cont'd)

- Parties involved in the data processing and the locations of the data processing.

| Process | Location | Controller | Processor & Sub-processor |
|---|---|---|---|
| Invite Traveller | the Netherlands (?) | KLM | ? |
| | | Air Canada | |
| Create KTDI Profile | ? (theoretically: everywhere) | ? | ?<br>Accenture |
| Create Digital ID | the Netherlands | KMar | NOID (Idemia) |
| Prepare the Trip | ? (theoretically: everywhere) | KLM | ? |
| | | Air Canada | ? |
| | | NOID | Idemia<br>Accenture |
| | | NCSC | AAS (Vision-Box) |
| | | KMar | AAS (Vision-Box) |
| Priority Access to security | the Netherlands | NCSC | AAS (Vision-Box) |
| Border Control NLD (ARR/DEP) | the Netherlands | KMar | AAS (Vision-Box) |
| Boarding Access | the Netherlands (?) | KLM/Air Canada | ?<br>AAS (Vision-Box) |

# Characteristics of Data Processing (cont'd)

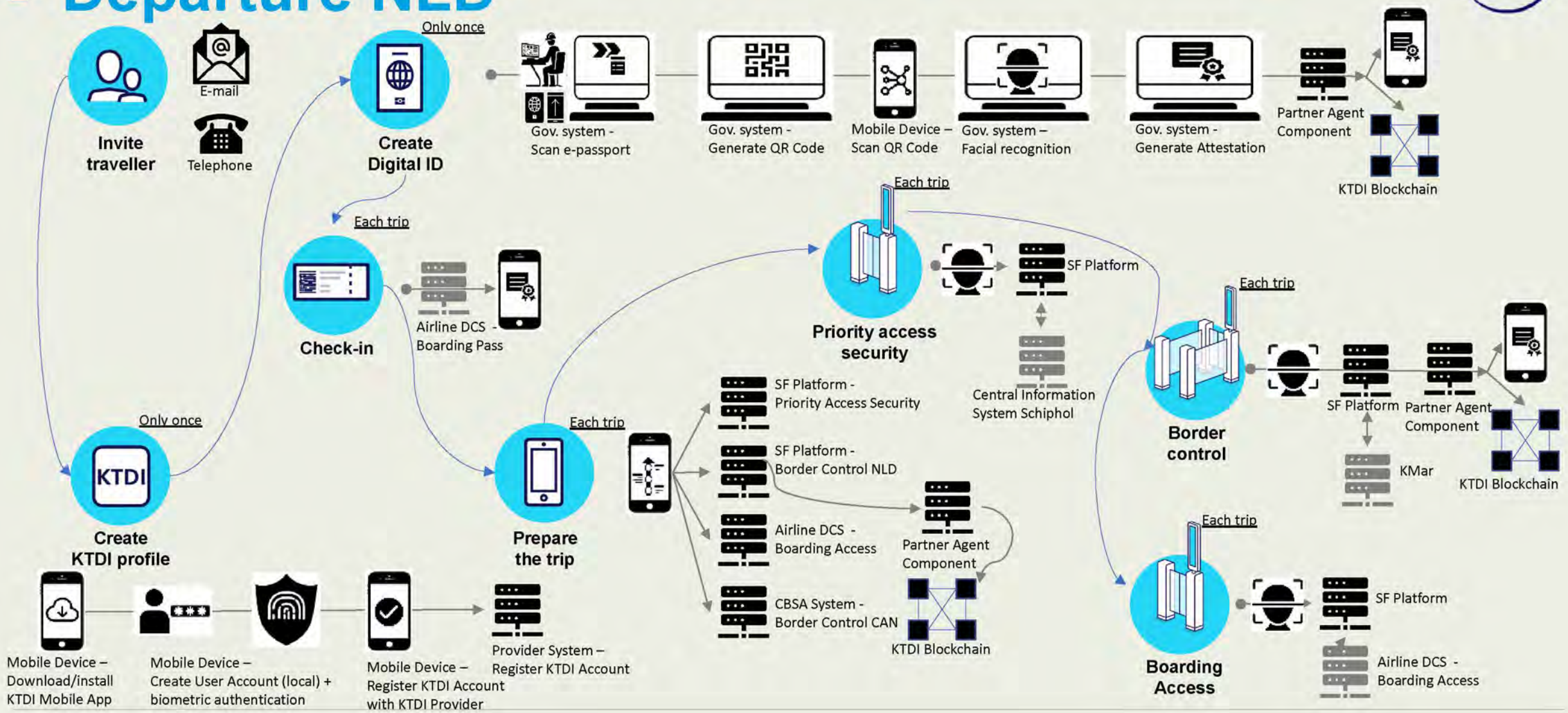
- Parties involved in the data processing and their interest in the data processing.

| Party | Role | Interest in the data processing |
|---|---|---|
| Air Canada | Controller | |
| KLM | Controller | |
| KMar | Controller | |
| NOID | Controller | |
| NCSC | Controller | |
| Accenture | Processor | |
| Idemia | Processor | |
| AAS | Processor | |
| Vision-Box | Processor | |
| ... | | |

# A.5 Characteristics of Data Processing

*Processes & Supporting Technology*

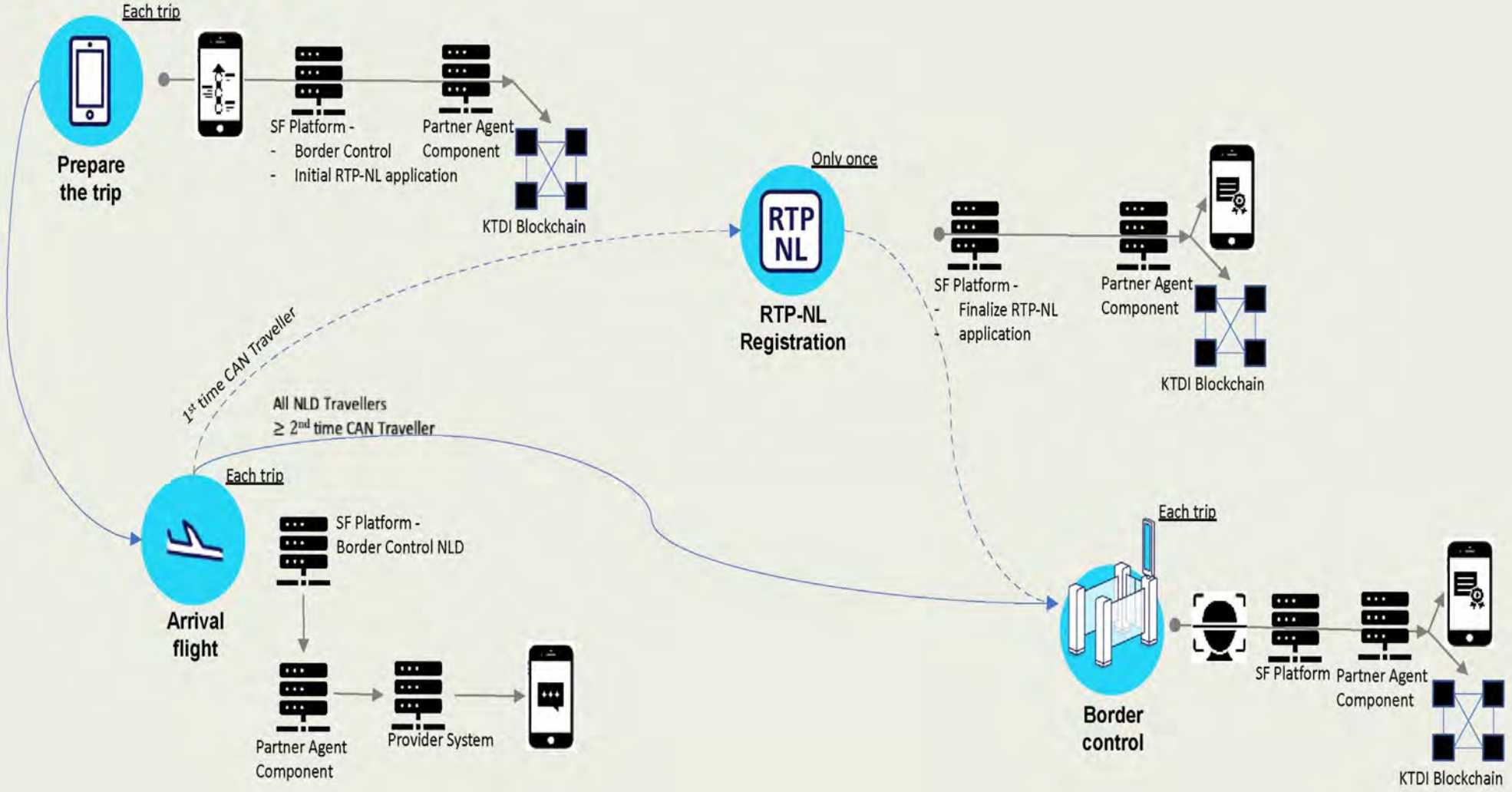
# KTDI Pilot Process & Supporting Technologies - Departure NLD



# KTDI Pilot Process & Supporting Technologies

—

## Arrival NLD



# A.5 Characteristics of Data Processing

## *Processes & Supporting Technology – Blockchain*

# Characteristics of Data Processing (cont'd) – some remarks about blockchain

- "Indeed, almost one year after the GDPR became binding and although the legal regime is largely based on the previous 1995 Data Protection Directive, it is evident that many pivotal concepts remain unclear."

- "It will be seen that the regulation is an expression of principles-based regulation that was designed to be technologically-neutral and stand the test of time in a fast-moving data-economy."

- "there is an ongoing debate surrounding whether data typically stored on a distributed ledger, such as public keys and transactional data qualify as personal data for the purposes of the GDPR. Specifically, the question is whether personal data that has been encrypted or hashed still qualifies as personal data. Whereas it is often assumed that this is not the case, such data likely does qualify as personal data for GDPR purposes…"

Source: Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law? (Secretariat of the European Parliament; Brussels 2019), pages i-iv.

# Characteristics of Data Processing (cont'd) – some remarks about blockchain

- "Whereas the GDPR requires that personal data that is processed be kept to a minimum and only processed for purposes that have been specified in advance, these principles can be hard to apply to blockchain technologies. Distributed ledgers are append-only databases that continuously grow as new data is added. In addition, such data is replicated on many different computers. Both aspects are problematic from the perspective of the data minimisation principle. It is moreover unclear how the 'purpose' of personal data processing ought to be applied in the blockchain context, specifically whether this only includes the initial transaction or whether it also encompasses the continued processing of personal data (such as its storage and its usage for consensus) once it has been put on-chain."

- "It is the tension between the right to erasure (the 'right to be forgotten') and blockchains that has probably been discussed most in recent years."

- "This analysis leads to two overarching conclusions. First, that the very technical specificities and governance design of blockchain use cases can be hard to reconcile with the GDPR. Therefore, blockchain architects need to be aware of this from the outset and make sure that they design their respective use cases in a manner that allows compliance with European data protection law. Second, it will however also be stressed that the current lack of legal certainty as to how blockchains can be designed in a manner that is compliant with the regulation is not just due to the specific features of this technology. Rather, examining this technology through the lens of the GDPR also highlights significant conceptual uncertainties in relation to the regulation that are of a relevance that significantly exceeds the specific blockchain context. Indeed, the analysis below will show that the lack of legal certainty pertaining to numerous concepts of the GDPR makes it hard to determine how the latter should apply both to this technology and to others."

Source: Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law? (Secretariat of the European Parliament; Brussels 2019), pages i-iv.

# A.6 Characteristics of Data Processing

*Miscellaneous*

# Characteristics of Data Processing (cont'd)

- Legal and policy framework:
  - Security: Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security, paragraph 1.2.2.1 – 1.2.2.4
  - Border Control: Schengen Borders Code.

- The KTDI mobile application does not support any back-up functionality.
  - Attestations will only be stored in the wallet of the KTDI mobile application and in databases of Service Providers which have requested them from the Traveller.
  - Data of non-core Building Blocks will only be stored in the wallet of the KTDI mobile application and in databases of Service Providers which have requested them from the Traveller.
- Retention periods:
  - These are not specific for or adapted to the KTDI concept.
  - During the pilot, statistical data will be collected as well as data on user experience/(dis-)satisfaction. This will be input for an evaluation of the KTDI concept.
    - Next steps are still to be defined.
- The KTDI pilot will last six months and can be prolonged for another six months. After that period, the pilot will be terminated and travellers can no longer make use of any KTDI related service.

# Data Processing

# Lawfulness of Data Processing

- Legal basis for data processing (GDPR, art. 6).

  - For Border Control: the Data Subject does not give consent for the data processing , a Data subject is under the legal obligation to have their passport checked. *
    - GDPR, article 6.1 (c): “processing is necessary for compliance with a legal obligation to which the controller is subject”; and
    - GDPR, article 6.1 (e): “processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”.

  - For Airlines (KLM, Air Canada), a Data Subject will have concluded a contract under which they are obliged to share certain personal data with the Airlines in order to make use of the KTDI Service ‘Boarding’.
    - GDPR, article 6.1(b): “processing is necessary for the performance of a contract to which the data subject is party …”
    - However: sharing the facial image is not part of the (current) contract between a Data Subject and the Airline. The Data Subject will need to give informed consent to the Airlines allowing them to process their facial image during the KTDI Service ‘Boarding’.
      - GDPR, article 6.1 (a): “the data subject has given consent to the processing of his or her personal data for one or more specific purposes”.

*) See: DPIA SSPC.

# Lawfulness of Data Processing (cont'd)

- Legal basis for data processing (GDPR, art. 6).
    - For the Airport, a Data Subject will have given informed consent to the processing of personal data by the airport so they can make use of the KTDI Service 'Priority Access to Security'.
        - GDPR article 6.1(a): "the data subject has given consent to the processing of his or her personal data for one or more specific purposes".
    - For RTP-NL Application a (Canadian) Data Subject will have given informed consent to the processing of personal data by the KMar so they can make use of the KTDI Service 'Cross NLD Border – Arrival'.
    - The Data Subject shares their personal data for every journey and within every journey for every KTDI Service they wish to make use of.
        - A 'subscription model' (subscribe once, use multiple times) is not envisioned for the KTDI pilot.
        - See document 'KTDI Pilot – Services' (Excel file).

# Lawfulness of Data Processing (cont'd)

- Is the data used for another goal than originally collected for (GDPR, art 6.4)?
    - Personal data is only collected for a specific KTDI Service:
        - 'Cross NLD Border (Departure/Arrival)'. Legal basis = the law;
        - 'Priority Access to Security '. Legal basis = informed consent;
        - 'Boarding' (the execution of the agreement between the airine and the Traveller.) Legal basis = the contract; and
            - Boarding using biometrics. Legal basis = informed consent.
        - 'RTP-NL Application'. Legal basis = informed consent.
    - The consent refers to giving the personal data via the KTDI mobile application to the relevant controllers in order to be able to make use of the KTDI services.
    - Concluding: no. The personal data, which is collected in order to enable a Data Subject to make use of a specific KTDI Service, is only used to provide that KTDI Service to the Data Subject.
- Necessity of data processing (GDPR, art. 6):
    - Proportionality of the data processing: data processing is based on the principle of 'Data Minimisation' (GDPR, art. 5.1.c). The data which is collected for a specific KTDI Service is limited to what is necessary in order to enable the Data Subject to make use of that KTDI Service.
- Subsidiarity: participation to the KTDI Pilot is on voluntary basis only. Dutch and Canadian Travellers who are invited to participate, may at all times refuse or terminate their participation. In that case, 'normal' border control facilities are available: Self-Sevice Passport Control and the manual counter.

# Lawfulness of Data Processing (cont'd)

- Rights of the data subject:
  - Information to be provided where personal data are collected from the data subject (GDPR, art. 13).
    - This information will be made available to the Data Subject at the time when the personal data are obtained.
    - The information will also be published on the web site of KTDI (www.ktdi.org).
  - Information to be provided where personal data have not been obtained from the data subject (GDPR, art. 14).
    - As far as applicable, this information will be published on the web site of KTDI (www.ktdi.org).
  - Right of access by the data subject (GDPR, art. 15).
    - A participating Traveller can ask the appropriate Controller access to their personal data.
  - Right of rectification (GDPR, art. 16).
    - A participating Traveller can ask the appropriate Controller to rectify their personal data.
  - Right of erasure (GDPR, art. 17).
    - NOID persistenly stores the digital identity of all participating [redacted]. If a participating [redacted] wishes to have their personal data deleted, they can request the NOID to do so. That does mean that the Dutch Traveller will not be able anymore to consume Dutch and Canadian KTDI Services.
    - Canadian participants who are member of the RTP-NL programme: see DPIA RTP-NL/3L.

# Lawfulness of Data Processing (cont'd)

- Rights of the data subject:
  - Right to restriction of processing (GDPR, art. 18).
    - A participating Dutch or Canadian Travellermay at all times invoke their right to restriction of processing by informing the appropriate Controller.
  - Right to data portability (GDPR, art. 20).
    - NOID persistenly stores the digital identity of all participating Travellers. If a participating wishes to transfer their personal data from NOID to any other organization, than they can request the NOID to supply them with the requested pesonal data.
    - The Royal Marechausseee persistently stores RTP-NL membership data of participating Travellers. If a participating wishes to transfer their personal data from the RTP-NL programme to any other organization, than they can request the Royal Marechaussee to supply them with the requested pesonal data.
    - Airlines: ?

# Lawfulness of Data Processing (cont'd)

- Rights of the data subject (cont'd):
  - Right to object (GDPR, art. 21).
    - The right to object is only applicable on data processing based on GDPR article 6.1(e) and 6.1(f):
      - Article 6.1(e): "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller".
      - Article 6.1.(f): "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data".
    - Making use of the KTDI Service 'Priority Access to Security' is based on informed consent (GPDR, article 6.1(a). Therefore, the right to object can not be executed while making use of this service.
    - Making use of the KTDI Service 'RTP-NL Application' is based on informed consent (GPDR, article 6.1(a). Therefore, the right to object can not be executed while making use of this service.
    - Making use of the KTDI Service 'Cross NLD Border (Departure and Arrival)' is based on public interest or the exercise of official authority vested in the controller (GPDR, article 6.1(a). Therefore, the right to object can be executed while making use of this service.
    - Making use of the KTDI Service 'Boarding' is based on a contract (GDPR, article 6.1(b) with the Participating Airline. The use of biometrics is based on informed consent. Therefore, the right to object can not be executed while making use of this service.

# Lawfulness of Data Processing (cont'd)

- Rights of the data subject (cont'd):
  - Automated individual decision-making, including profiling (GDPR, art. 22).
    - Not applicable to the KTDI Pilot.
    - See DPIA of:
      - Seamless Flow; and
      - RTP-NL/3L.
    - Airlines: ?

# C./D. – Risks & Mitigation

# Risks & Mitigations - Introduction

In this chapter, risks are described which a Data Subject may run as they travel the 'KTDI way', including:

- The negative consequences which the Data Subject may experience;
- The source of these consequences;
- The possibility that these risks may occur; and
- The impact of the risk on the Data Subject. The impact is assessed taking into account: loss of freedom, are special categories of personal data processed , can the Data Subject experience financial damage.

For each risk, mitigating measures are identified and described in this chapter as well.

- A mitigating measure can be of a technological, organizational or legal nature.
- It may very well be possible that parts of a risk are not covered by the measures. In these cases, it will be explained why those residual risks are acceptable.

# Risks with regard to the KTDI Mobile Application

| GDPR Principle | Privacy Risks | Mitigations |
|---|---|---|
| Lawfulness, fairness and transparency Art.5(1)(a) | Unlawful, excessive and incorrect processing (e.g. due to permissions to unauthorised parties to access personal data through the app). | App providers/developers should make sure that they have a legal basis for the processing of personal data.<br>App providers/developers should inform the data subjects properly about their data processing activities. This may help the users to understand what personal data is collected by them and why.<br>App providers/developers should be aware of data subject rights such as rights to access, rectification, erasure, data portability. They should implement appropriate processes to support these rights |
| Purpose limitation Art.5(1)(b) | Excessive collection and sharing of data (e.g. due to multiple sensors of mobile devices that are activated without need). | App providers/developers should use the data for a specific purpose that the data subjects have been made aware of and no other, without further consent. If the personal data is used for purposes other than the initial, they should be anonymised or the data subjects must be notified and their consent must be re-obtained. |
| Data minimisation Art.5(1)(c) | Excessive processing (e.g. due to use of third party libraries). | The minimum amount of data for specific processing should be processed by app providers/developers. For instance, they should not store the exact location point when a generic location area is sufficient for their app functionalities.<br>**Measures**:<br>• The KTDI Mobile Application must only process data which are absolutely necessary for a user to make use of a KTDI Service.<br>• The KTDI Mobile Application must not collect geolocaton data. |
| Accuracy Art.5(1)(d) | Outdated data pose identity theft risks. | Rectification processes into data management should be embedded in the app design. |

Sources: Privacy and data protection in mobile applications (ENISA; november 2017), page 22; Smartphone Secure Development Guidelines (ENISA; december 2016).

# Risks with regard to the KTDI Mobile Application cont'd

| GDPR Principle | Privacy Risks | Mitigations |
|---|---|---|
| Storage limitation Art.5(1)(e) | Undue data disclosure (e.g. due to cloud storage services used by mobile app developers). | Personal data must not be stored longer than necessary. App providers/developers should provide the "right to be forgotten" to the data subjects. This data must be kept only for a certain period of time for non-active users.<br>**Measures:**<br>• The KTDI Mobile Application & Wallet must not persistenly store Attestations issued by NOID containing persona data. These Attestations (and other objects in the cache of the app) must be irrevocably deleted after:<br>  • xx seconds of idle time; or<br>  • The Traveller has terminated the KTDI Mobile Application. |

Sources: Privacy and data protection in mobile applications (ENISA; november 2017), page 22; Smartphone Secure Development Guidelines (ENISA; december 2016).

# Risks with regard to the KTDI Mobile Application cont'd

| GDPR Principle | Privacy Risks | Mitigations |
|---|---|---|
| Integrity and confidentiality Art.5(1)(f) | Unlawful data processing,<br>data loss, data breach,<br>data destruction or damage | App providers/developers should ensure that the security requirements of the personal data and the processing systems are met. This encompasses integrity and confidentiality as well as availability and resilience (Art. 35(1)(b) GDPR). For instance, the appropriate control access mechanisms should be embedded into the apps infrastructure in order to detect or monitor unauthorized access to the data.<br>**Measures:**<br>• Data at rest must be encrypted using a state-of-the-art encryption.<br>• Data at transport must be encrypted using a state-of-the-art encryption.<br>• The KTDI Mobile Application may nog have a 'debug mode' or 'developper mode'.<br>• The password of the user account must follow a strong password policy.<br>• The password must be masked while the user enters it in an input field.<br>• The password of the user account must be securely stored on the mobile device, making use of encryption and key-store mechanisms provided by the mobile OS. |

Sources: Privacy and data protection in mobile applications (ENISA; november 2017), page 22; Smartphone Secure Development Guidelines (ENISA; december 2016).

# Risk – Data Subject cannot execute their rights

| Risk | Data Subject cannot execute their rights |
|---|---|
| Description | The Data Subject cannot execute their rights. KTDI's data processing is complex because multiple organisations are involved. Some of them are based within the EU, some outside of the EU. Data processing can happen within the EU, but also outside of the Data Subject could also choose to make use of a KTDI Service by accident.<br><br>This can be caused by:<br>• Unclear information.<br>• Unclear agreements between controllers and processors. |
| Possibility | Currently, there are no data processing agreements between Data Controllers and Data Processors. Before the actual pilot will start, these agreements must be concluded. That may solve the issue of unknown data processing. However, due to the complex nature of the KTDI processes, it may very well be that Data Subjects do not fully understand the KTDI concept, the possible consequences of the concept to their rights and how they execute their rights in relation with the KTDI concept.<br><br>• The possibility that this risk may occur is 'high'. |
| Impact | |

# Risk – Data Subject cannot execute their rights - cont'd

| Risk | Data Subject cannot execute their rights |
|---|---|
| Mitigation | • Terms and Conditions will be made available in gthe KTDI mobile application, KTDI web site, web site of Service Providers.<br>  • Including a clear desciption how a Traveller can execute his rights.<br>• A clear Processing Agreement must be concluded between each Controller and their Processor(s) before the actual pilot starts. |

| Possibility | Impact | Risk before implementation of mitigating measures | Risk after implementation of mitigating measures |
|---|---|---|---|
|  |  |  |  |

# Risk – Stigmatization & Discrimination

| Risk | Stigmatization & Discrimintion |
|---|---|
| Description | Personal data (biographic as well as biometric) can fall into the wrong hands and be used in order to discriminate of stigmatize the Data Subject. It is also possible that a Data Subject who has enrolled into KTDI and wants to make use of KTDI Services cannot be recognized by a touchpoint and will be referred to manual processing causing negative feelings. Also, it has been proofed that matching algorithms may have difficulties recognizing dark coloured skins which may also cause negative feelings.<br><br>This can be caused by:<br>• Data leakage.<br>• System errors.<br>• Unclear agreements about data processing (access to personal data).<br>• Function creep which caused personal data to be processed for other purposed than collected for. |
| Possibility | Service Providers and Information Systems used in the KTDI pilot must comply with security measures according to international standards (ISO, OWASP) but unfortunately a data leakage or system error cannot be ruled out completely.<br>Currently, there are no data processing agreements between Data Controllers and Data Processors. Before the actual pilot will start, these agreements must be concluded. That may solve the issue of unwanted data processing.<br><br>• The possibility that this risk may occur is 'medium'. |
| Impact | A Data Subject could experience discrimination or stigmatization. As a result of a system error the Data Subject may inadvertently be denied border crossing or boarding possibly even resulting in the Data Subject missing their flight.<br><br>• The impact of this risk is 'high'. |

# Risk – Stigmatization & Discrimintion - cont'd

| Risk | Stigmatization & Discrimintion |
|---|---|
| Mitigation | • Each Controller and Processor must have a procedure in place how to act in case of data leakage or system error.<br>• Each Controller and Processor must demonstrable comply to international Information Security standards.<br>• A clear Processing Agreement must be concluded between each Controller and their Processor(s) before the actual pilot starts.<br>• Each Controller and Processor must only process data for the purpose the data was collected for.<br>• Audits may be executed in order to verify if a Controller or Processor has implemented the above mentioned measures. |

| Possibility | Impact | Risk before implementation of mitigating measures | Risk after implementation of mitigating measures |
|---|---|---|---|
|  |  |  |  |

# Risk – Adverse decision taking due to erroneous data

| Risk | Adverse decision taking due to erroneous data |
|---|---|
| Description | A Service Provider could take a decision based on erroneous data. This has a negative impact on the Data Subject.<br><br>This can be caused by:<br>• Erroneous record keeping: data of a Data Subject is combined with data of another Data Subject. |
| Possibility | • The possibility that this risk may occur is 'medium'. |
| Impact | A Data Subject could experience negative feelings discrimination or stigmatization. As a result of a system error the Data Subject may inadvertently be denied border crossing or boarding possibly even resulting in the Data Subject missing their flight.<br><br>• The impact of this risk is 'high'. |

# Risk – Adverse decision taking due to erroneous data - cont'd

| Risk | Adverse decision taking due to erroneous data |
|---|---|
| Mitigation | • Controllers need to implement measures guaranteeing data integrity. |

| Possibility | Impact | Risk before implementation of mitigating measures | Risk after implementation of mitigating measures |
|---|---|---|---|
|  |  |  |  |