WORLDWIDE AIRPORTS LAWYERS ASSOCIATION

WELCOME TO WALA X

London, UK
October 15-17, 2018

A “Common-Use” Proposal for GDPR at Airports

Jonas Bartlett & Navdeep Gill

SITA

17 October 2018

Contents

Background – Common Use IT @ Airports

The "GDPR Problem"
– in "non-CLUB Model" Common Use situations

The "Data Supply Chain" & GDPR

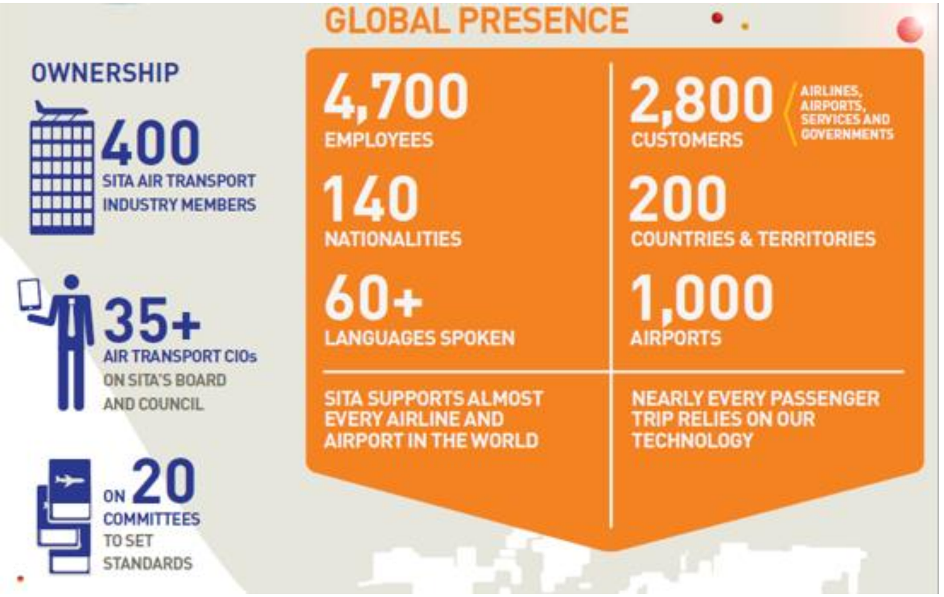
A Potential Solution for Airports & Benefits

Templates & GDPR Background

Host

YOUR LONDON AIRPORT
Gatwick

About SITA



GLOBAL PRESENCE

OWNERSHIP

400 SITA AIR TRANSPORT INDUSTRY MEMBERS

35+ AIR TRANSPORT CIOs ON SITA'S BOARD AND COUNCIL

ON **20** COMMITTEES TO SET STANDARDS

4,700 EMPLOYEES

2,800 CUSTOMERS (AIRLINES, AIRPORTS, SERVICES AND GOVERNMENTS)

140 NATIONALITIES

200 COUNTRIES & TERRITORIES

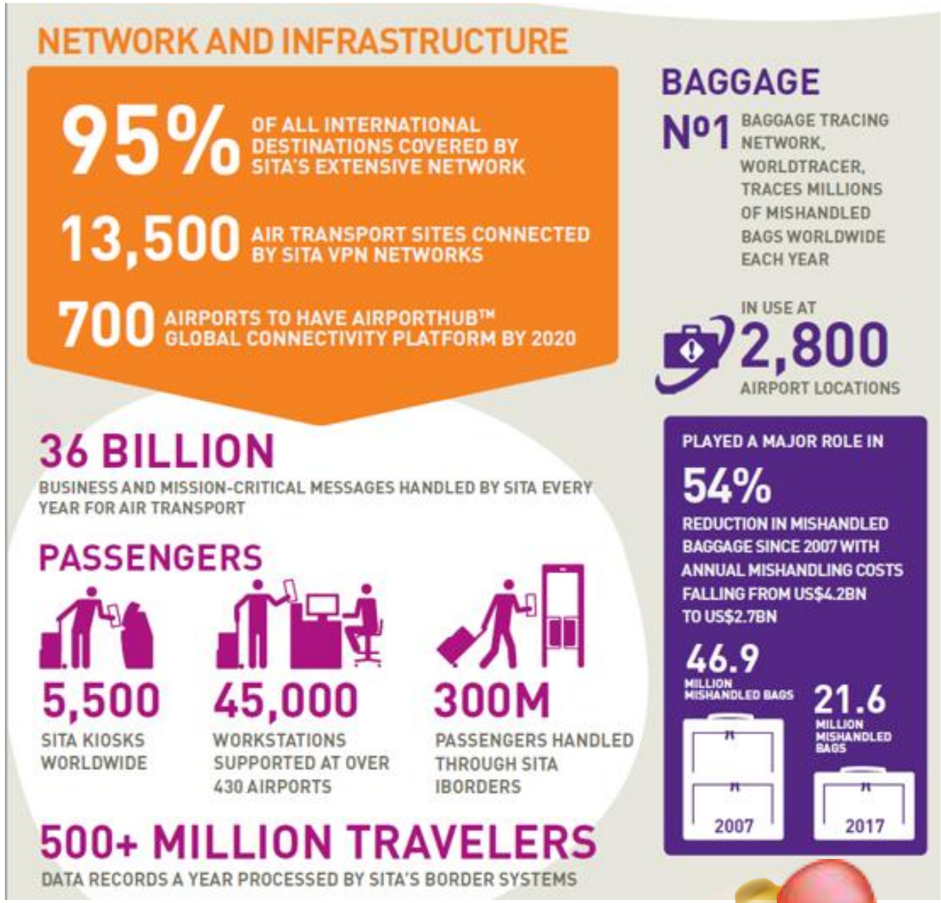
60+ LANGUAGES SPOKEN

1,000 AIRPORTS

SITA SUPPORTS ALMOST EVERY AIRLINE AND AIRPORT IN THE WORLD

NEARLY EVERY PASSENGER TRIP RELIES ON OUR TECHNOLOGY

SITA



NETWORK AND INFRASTRUCTURE

95% OF ALL INTERNATIONAL DESTINATIONS COVERED BY SITA'S EXTENSIVE NETWORK

13,500 AIR TRANSPORT SITES CONNECTED BY SITA VPN NETWORKS

700 AIRPORTS TO HAVE AIRPORTHUB™ GLOBAL CONNECTIVITY PLATFORM BY 2020

36 BILLION

BUSINESS AND MISSION-CRITICAL MESSAGES HANDLED BY SITA EVERY YEAR FOR AIR TRANSPORT

PASSENGERS

5,500 SITA KIOSKS WORLDWIDE

45,000 WORKSTATIONS SUPPORTED AT OVER 430 AIRPORTS

300M PASSENGERS HANDLED THROUGH SITA IBORDERS

500+ MILLION TRAVELERS

DATA RECORDS A YEAR PROCESSED BY SITA'S BORDER SYSTEMS

BAGGAGE

Nº1 BAGGAGE TRACING NETWORK, WORLDTRACER, TRACES MILLIONS OF MISHANDLED BAGS WORLDWIDE EACH YEAR

IN USE AT **2,800** AIRPORT LOCATIONS

PLAYED A MAJOR ROLE IN

54% REDUCTION IN MISHANDLED BAGGAGE SINCE 2007 WITH ANNUAL MISHANDLING COSTS FALLING FROM US$4.2BN TO US$2.7BN

SITA

Background – Common Use IT @ Airports

The “GDPR Problem”
– in “non-CLUB Model” Common Use situations

The “Data Supply Chain” & GDPR

A Potential Solution for Airports & Benefits

Templates & GDPR Background

Host

YOUR LONDON AIRPORT
Gatwick

What is Shared-use / Common-use?

- Infrastructure/equipment that is used by multiple airlines/GHAs, and contracted by those airlines/GHAs.
- First occurred in 1980s (by SITA @ Los Angeles, for 1984 Olympics).

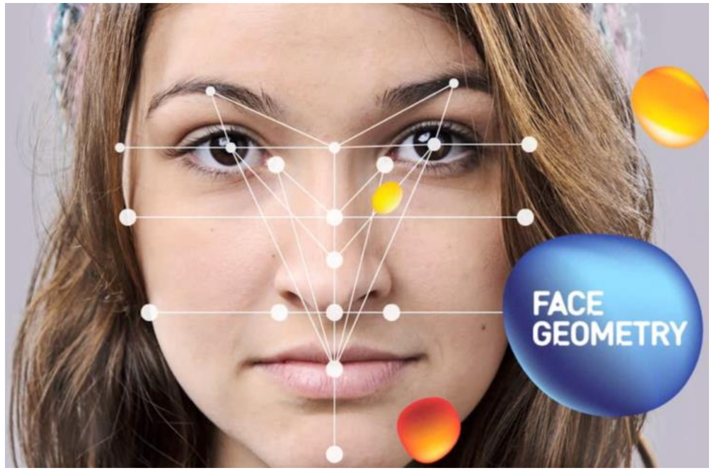
- Many things can be supplied this way:

  Long-term:

  - Check-in desks / peripherals / kiosks

  New:

  - Biometric systems – check-in/entry/exit
  - Self-service bag drop machines
  - Self-boarding & security gates
  - P2PE payment devices



(No MSRs for credit cards!)

What are “CLUBs?”

- **CUTE® What is it?** “Common Use Terminal Equipment”.
- **CLUB. What is it?** A group of airlines and Ground Handlers, each as an entity on its own behalf, who sign an agreement with SITA for shared services, on the basis of equal service treatment.
  - SITA will have a concession from the airport.
  - CUTE equipment / infrastructure is usually owned & operated by SITA.
- **A “Common-use Local User Board” (CLUB)** is formed by the airlines & GHAs to manage the shared systems at the site.
  - ***STANDARDIZED CONTRACTS APPLY*** - service contract & “terms of reference”
  - A CLUB Chairperson is elected. Informal structure governed by agreed contractual rules and processes.

Legal Models for Shared-use Supply

Common Use – “CLUB”* model

Airlines/GHAs buy services as a group/ committee.

ADVANTAGES:
Airport has no operational liability. Airport is free to sell additional services.

DISADVANTAGES:
Airport cannot control service.

HYBRID – “Airport joins CLUB Option”

“CLUB” model but airport joins the group as a non-fee paying committee member.

ADVANTAGES:
Enhanced collaboration. Airport can influence committee and has voting power – veto voting power possible.

DISADVANTAGES:
Airport is not in full control as in “Direct” model.

Airport Sourcing – “Direct” model

Airport buys services, resells to airlines/GHAs.

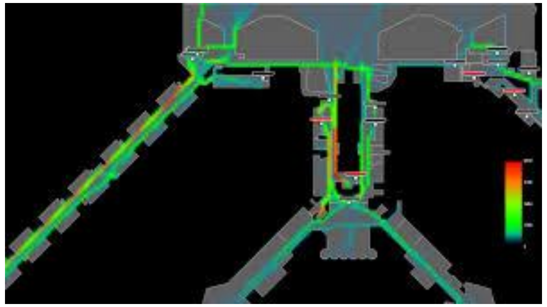
ADVANTAGES:
Airport is in full control as sole reseller of service to airlines/GHAs

DISADVANTAGES:
Airport is liable to airlines/GHAs as service provider.

Less used than other models today – but useful if airport seeks to retain a level of control / influence while avoiding full liability of “Direct” model

*** CLUB stands for “Common-use Local Users Board”. (Not a legal entity.)**

What is the future for shared-use?



- Shared-use IT infrastructure in airports is convenient and efficient.

- BUT: The long-term trend is for less shared use, and more “direct” IT service resale by airports.

  → Why?

  → Does data security influence this?

- What do airports need to be aware of in the “direct” model?

Recent Data Breaches in Air Transport (not in shared-use environments)

- August 2018: A large North American airline:

Data breach on mobile app affecting up to 20,000 people. Attackers may have accessed basic profile data, including names, email addresses and phone numbers — and passport numbers and expiry date, passport country of issuance, NEXUS numbers for trusted travelers, gender, dates of birth, nationality and country of residence. All accounts re-set.

- September 2018: A large European airline:

380,000 customers had personal data accessed. The hackers obtained names, street and e-mail addresses, and credit-card numbers, expiry dates and security codes, potentially enabling them to steal money from bank and credit-card accounts. The airline promised compensation for any customers financially affected. Hackers may have breached the system that managed customer payments.

Background – Common Use IT @ Airports

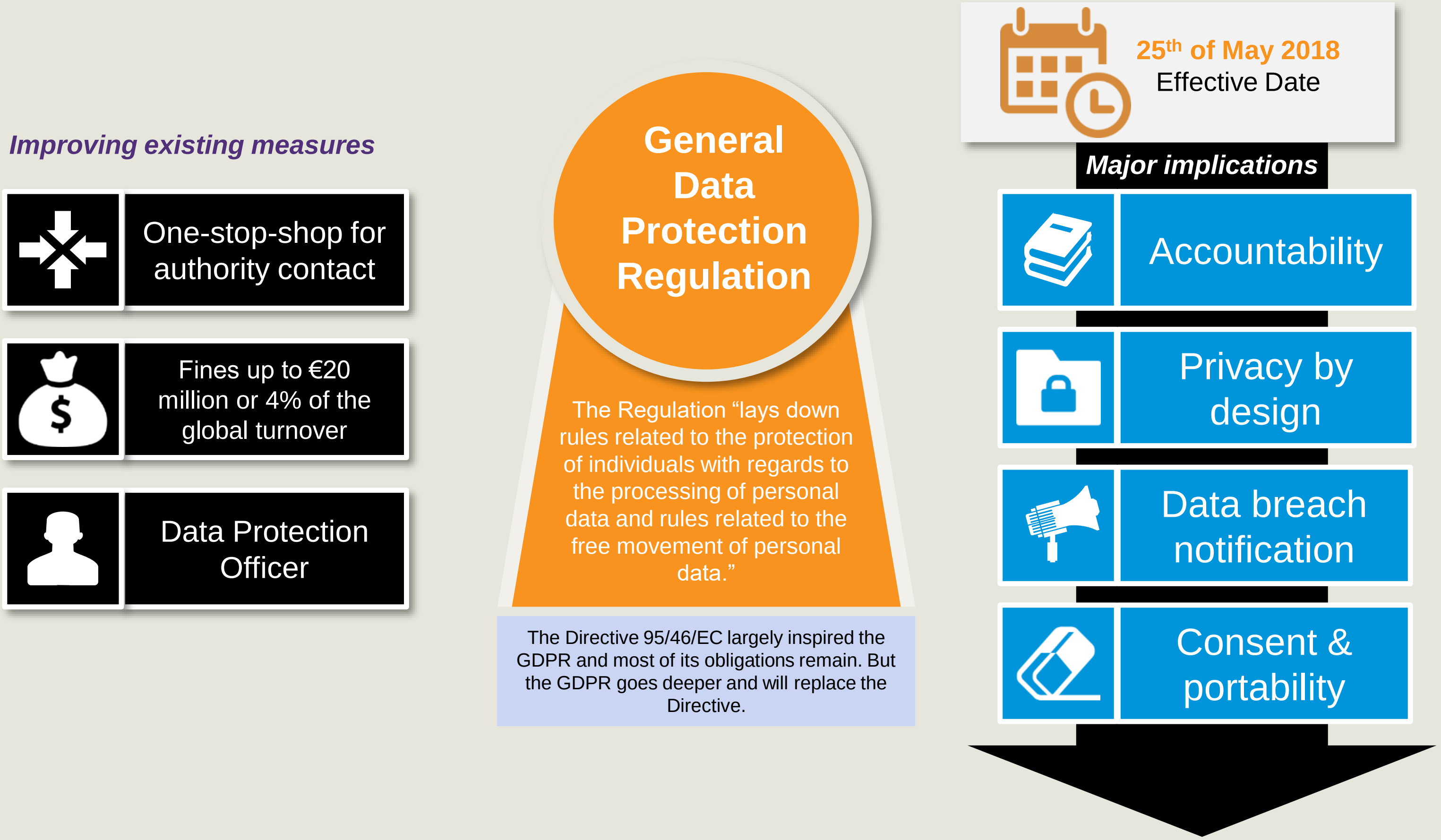
The "GDPR Problem"
– in "non-CLUB Model" Common Use situations

The "Data Supply Chain" & GDPR

A Potential Solution for Airports & Benefits

Templates & GDPR Background

EU Regulation 2016/679 - the GDPR - in a nutshell



Improving existing measures

One-stop-shop for authority contact

Fines up to €20 million or 4% of the global turnover

Data Protection Officer

General Data Protection Regulation

The Regulation "lays down rules related to the protection of individuals with regards to the processing of personal data and rules related to the free movement of personal data."

The Directive 95/46/EC largely inspired the GDPR and most of its obligations remain. But the GDPR goes deeper and will replace the Directive.

25th of May 2018

Effective Date

Major implications

Accountability

Privacy by design

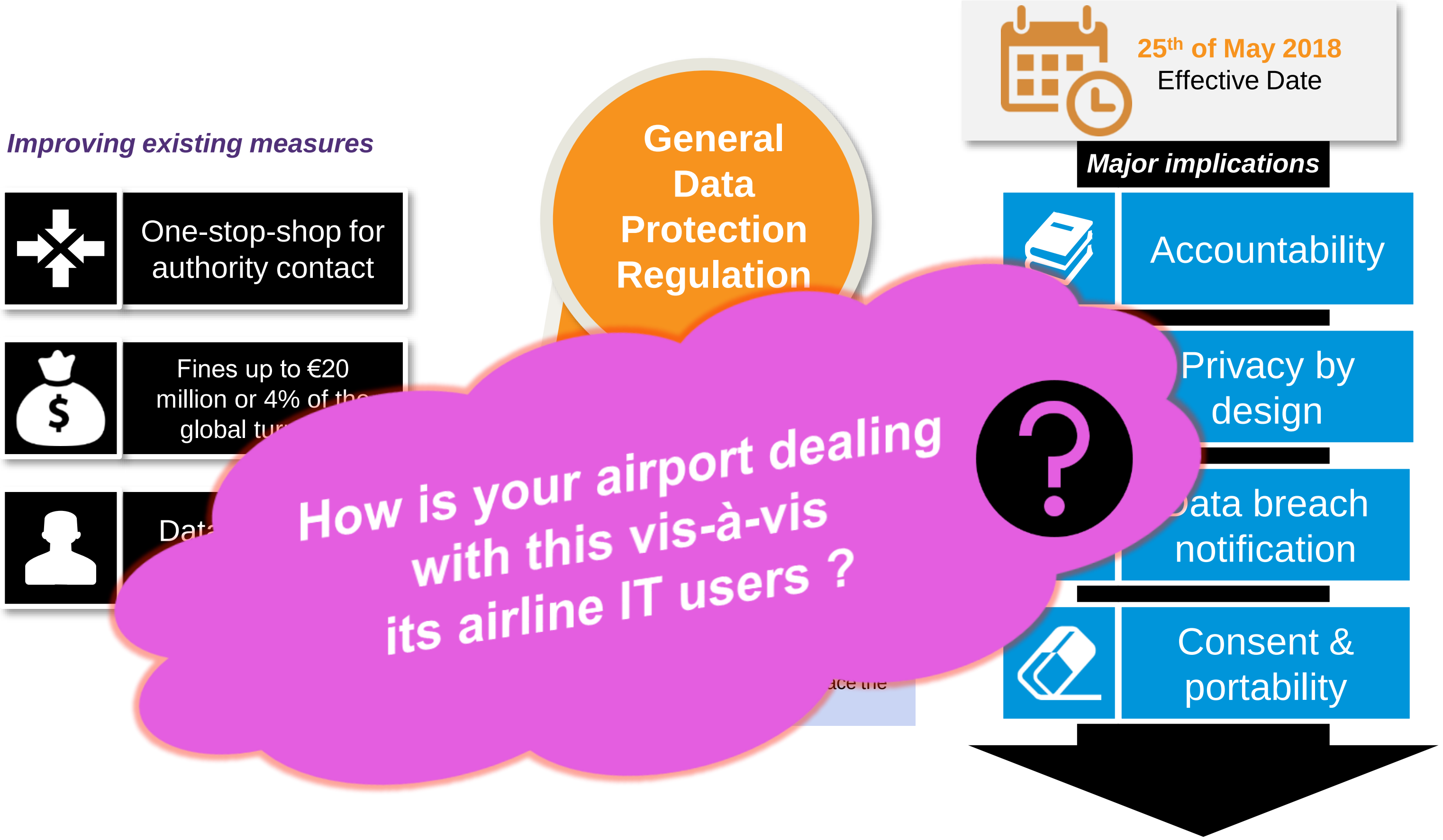
Data breach notification

Consent & portability

Graphics by SITA's partner

WAVESTONE

EU Regulation 2016/679 - the GDPR - in a nutshell



Improving existing measures
One-stop-shop for authority contact
Fines up to €20 million or 4% of the global tu
Dat
General Data Protection Regulation
ace the
25th of May 2018
Effective Date
Major implications
Accountability
Privacy by design
ata breach notification
Consent & portability

How is your airport dealing with this vis-à-vis its airline IT users ?

Graphics by SITA's partner

WAVESTONE

THE “GDPR PROBLEM” FOR AIRPORTS

- Many airports resell CUTE/CUPPS/CUSS solutions to airlines. We could call this the “direct” or “non-CLUB” resale Airport Model
- GDPR imposes obligations on “controllers” and “processors” of *personal data of EU citizens.* The Airlines/GHAs will be “data controllers”, and they will seek to pass obligations to their suppliers – ***including Airports***
- Fines & liabilities can be major. Liability protection and legal clarity for all parties is desirable
- If a non-uniform approach is taken by different airports and airlines, then divergence in approach is inevitable

Background – Common Use IT @ Airports

The “GDPR Problem”
– in “non-CLUB Model” Common Use situations

The “Data Supply Chain” & GDPR

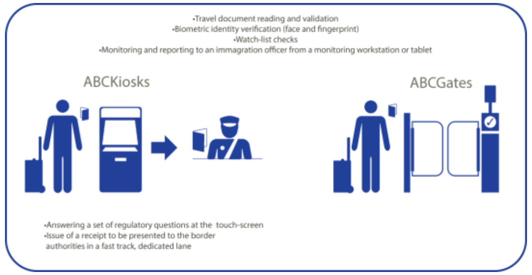
A Potential Solution for Airports & Benefits

Templates & GDPR Background

Host

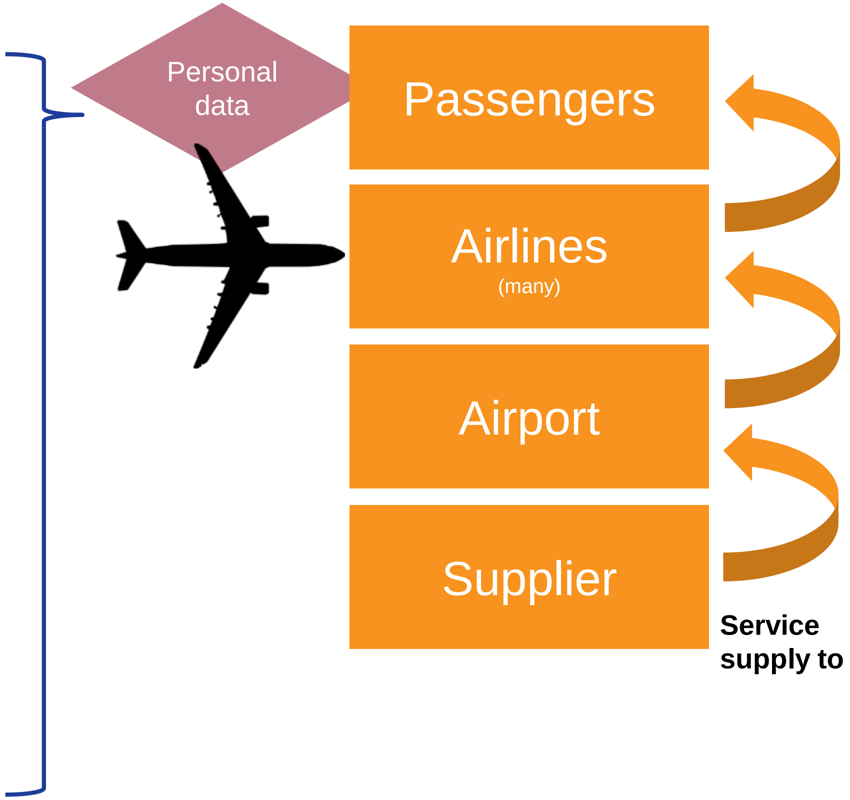
YOUR LONDON AIRPORT
Gatwick

THE “DATA SUPPLY CHAIN” @ AN AIRPORT – AN EXAMPLE



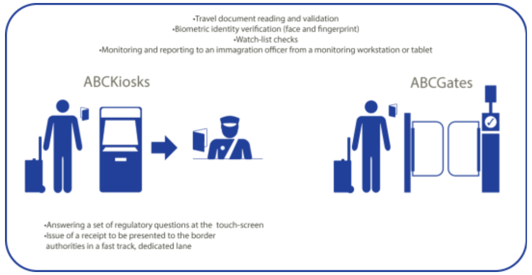
- Travel document reading and validation
- Biometric identity verification (face and fingerprint)
- Watch-list checks
- Monitoring and reporting to an immagration officer from a monitoring workstation or tablet

- Answering a set of regulatory questions at the touch-screen
- Issue of a receipt to be presented to the border authorities in a fast track, dedicated lane



Service supply to

THE “DATA SUPPLY CHAIN” @ AN AIRPORT – AN EXAMPLE

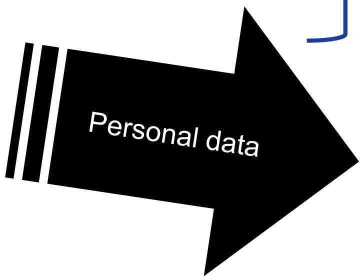


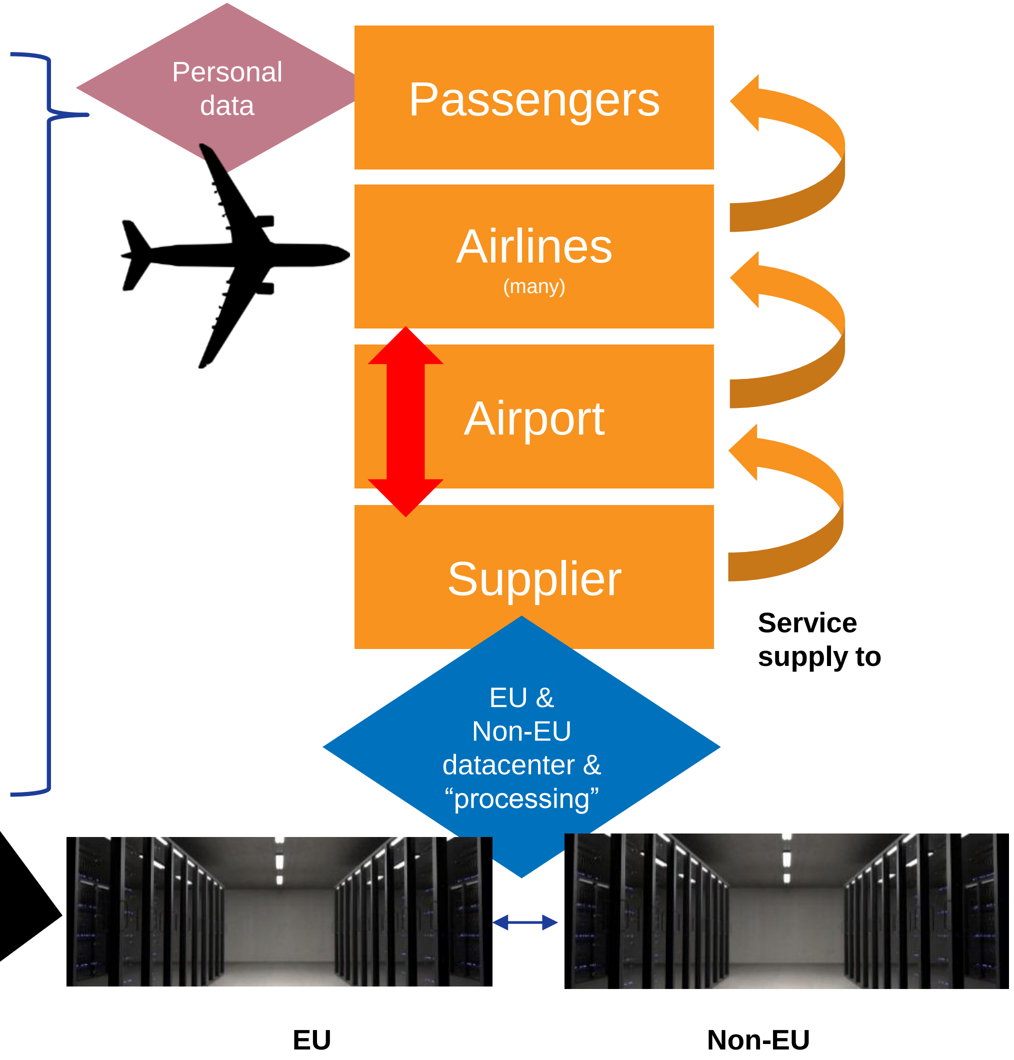
- Travel document reading and validation
- Biometric identity verification (face and fingerprint)
- Watch-list checks
- Monitoring and reporting to an immagration officer from a monitoring workstation or tablet

ABCKiosks

ABCGates

- Answering a set of regulatory questions at the touch-screen
- Issue of a receipt to be presented to the border authorities in a fast track, dedicated lane





The “Data + GDPR problem” for Airports

Two questions now arise for each affected Airport:

A. What GDPR contractual terms will it agree with its common use suppliers who have access to pax personal data? (SITA etc)

B. What GDPR contractual terms will it agree with airlines (the customers) using common use?

A potential solution is **standardization** of approach on an airport-wide basis.

SITA

Background – Common Use IT @ Airports

The "GDPR Problem"
– in "non-CLUB Model" Common Use situations

The "Data Supply Chain" & GDPR

A Potential Solution for Airports & Benefits

Templates & GDPR Background

Host

YOUR LONDON AIRPORT
Gatwick

A potential solution for airports

How would it work?

A. What GDPR terms will each Airport agree with its re-supplied suppliers who have access to pax personal data? (SITA etc)

→ *ANSWER: VOLUNTARY STANDARD TERMS AGREED "IN PRINCIPLE" FOR SUPPLIERS BY A WORKING GROUP – THEN ROLLED OUT TO EACH AIRPORT & SUPPLIER AGREEMENT (THE "UNIFORM SUPPLIER TERMS") AS & WHEN VOLUNTARILY AGREED (NOT MANDATORY)*

B. What GDPR terms will each Airport agree with airlines (the customers) using the IT service?

→ *ANSWER: BACK-TO-BACK OF THE "UNIFORM SUPPLIER TERMS", ROLLED OUT UNIFORMLY TO EACH AIRLINE – AGAIN, NOT MANDATORY – OFFERED AS A "SHORT CUT" FOR EASE OF CONTRACTING*

Deviations in the "Uniform Supplier Terms" for GDPR would be possible, but ideally limited, in order to achieve the benefits of a standard & back-to-back approach.

Benefits

Benefits of a standardized approach:

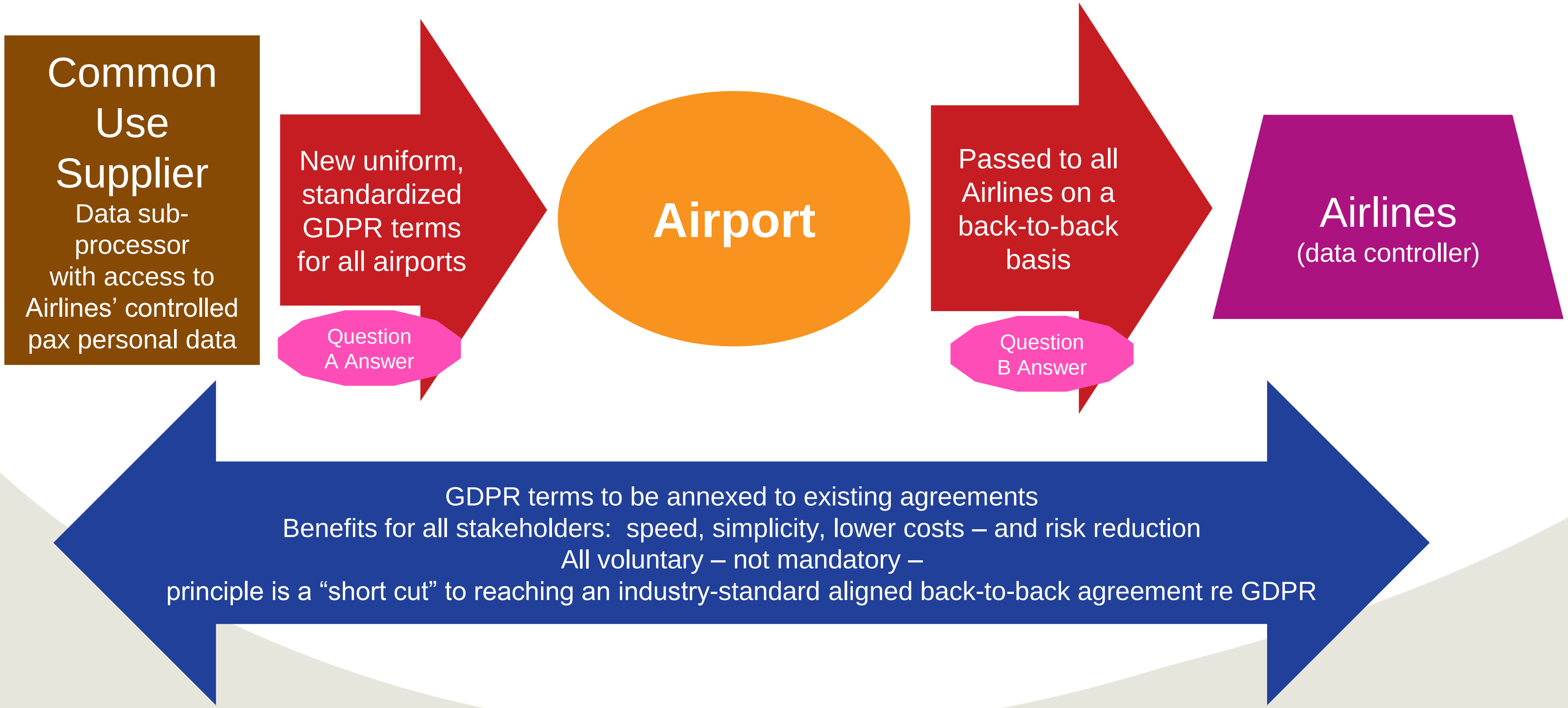
- Airports would be protected by back-to-back terms from suppliers
- A simplified approach for all stakeholders – with lower legal fees
- Potentially leading to a majority of contracts with GDPR coverage by mid-2018
- All leading to greater clarity and lower risk

RE-CAP: A POTENTIAL SOLUTION

Suggested templates for each

for possible stakeholder review included in back-up slide

Answers are proposed as follows:


Common Use Supplier
Data sub-processor with access to Airlines' controlled pax personal data
New uniform, standardized GDPR terms for all airports
Question A Answer
Airport
Passed to all Airlines on a back-to-back basis
Question B Answer
Airlines
(data controller)

GDPR terms to be annexed to existing agreements
Benefits for all stakeholders: speed, simplicity, lower costs – and risk reduction
All voluntary – not mandatory –
principle is a "short cut" to reaching an industry-standard aligned back-to-back agreement re GDPR

Can it work ? → YES !

- This is not "too optimistic" – this can work.
- Standardization of contracts has worked successfully for CLUBS for 35 years !

- SITA is available to join a working group to assist to create standardized documents.

- SITA has shared this idea with the ACI and feedback is positive – idea presented to:
  - ACI Facilitation & Customer Services Committee – Cyprus – 4 May 2018
  - ACI World Airport Information Technology Standing Committee (WAITSC) – Rio – 15-16 May 2018

AIRPORTS COUNCIL INTERNATIONAL

SITA

Background – Common Use IT @ Airports

The “GDPR Problem”
– in “non-CLUB Model” Common Use situations

The “Data Supply Chain” & GDPR

A Potential Solution for Airports & Benefits

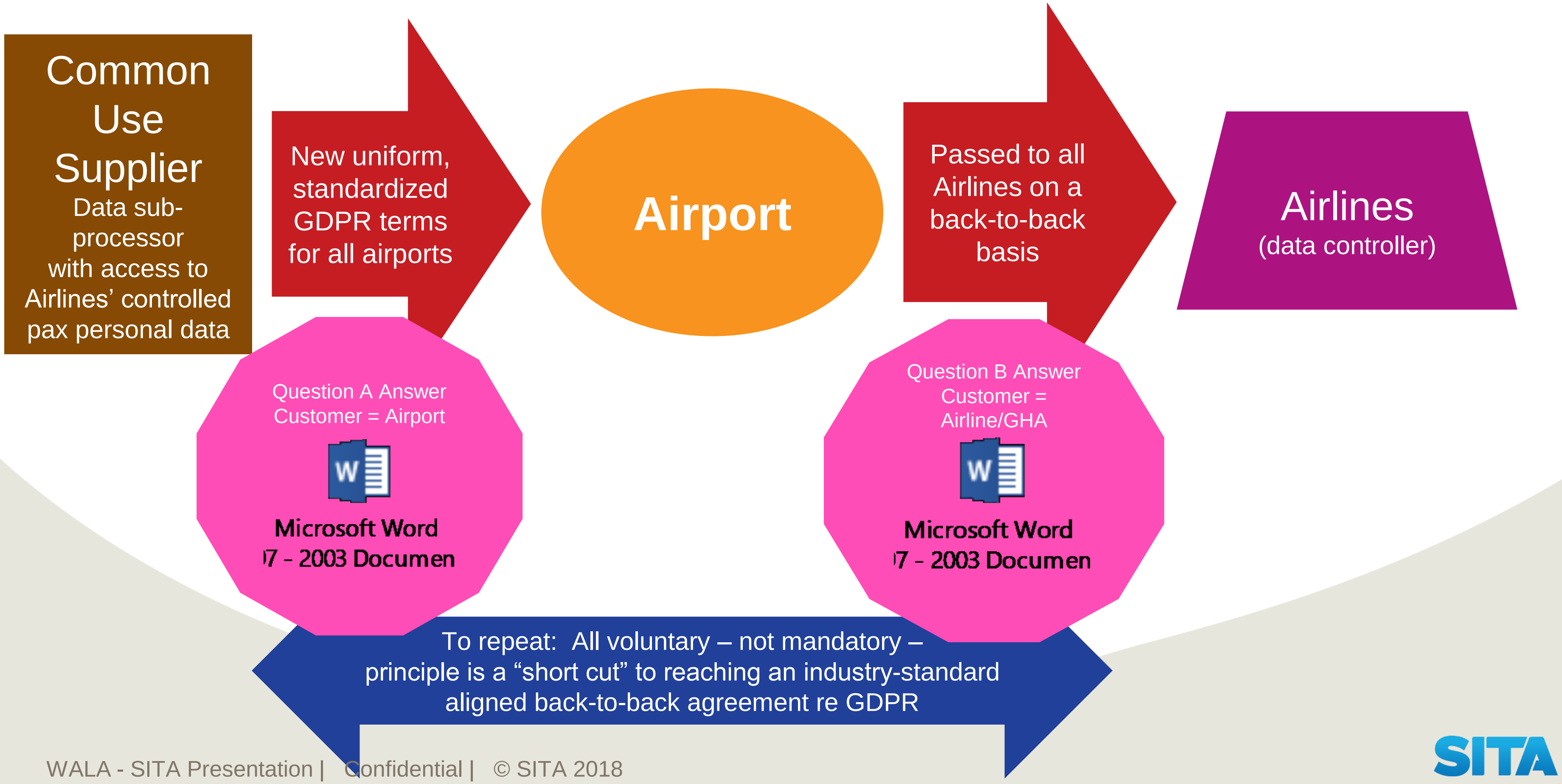
Templates & GDPR Background

Host

YOUR LONDON AIRPORT
Gatwick

RE-CAP: A POTENTIAL SOLUTION –

SUGGESTED TEMPLATES – FOR REVIEW – ARE IN WORD FORMAT, EMBEDDED HERE



Common Use Supplier
Data sub-processor
with access to
Airlines' controlled
pax personal data

New uniform, standardized GDPR terms for all airports

Airport

Passed to all Airlines on a back-to-back basis

Airlines
(data controller)

Question A Answer
Customer = Airport

Microsoft Word
7 – 2003 Documen

Question B Answer
Customer = Airline/GHA

Microsoft Word
7 – 2003 Documen

To repeat: All voluntary – not mandatory –
principle is a "short cut" to reaching an industry-standard
aligned back-to-back agreement re GDPR

PERSONAL DATA – DEFINITION

What is Personal data?

- Any information relating to a directly or indirectly identifiable individual (the “data subject”). Includes obviously personal data – e.g. name, contact details, identification number, etc.

- Also less obviously personal data – e.g. IP addresses, cookies etc. and generally any information specific to a person’s physical, physiological, mental, economic, cultural or social identity.

- It is a subjective test and therefore the definition of personal data is very broad.

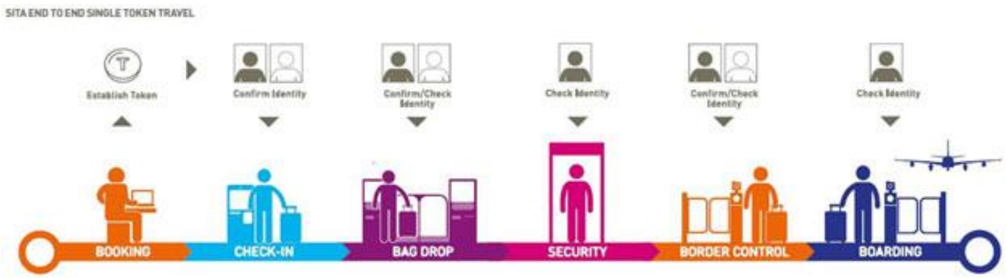
(Differs from the definition of Personally Identifiable Information (PII) in the US which only deals with data that actually identifies a person as compared with data that is identifiable, eg in Europe location data or online identifiers like web tracking tools would be classified as Personal Data, whereas in the US it would not.)

PERSONAL DATA – DEFINITION

Potentially –
any data enabling
“personalization” –
like this

Building brand loyalty through personalised offers
Tailored offers provided based on passenger online behaviour

PROCESSING RIGHT



There must be a lawful reason for Processing of pax data, such as:

- Consent of the data subject / passenger; or
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract; or
- Processing is necessary to comply with a legal obligation.

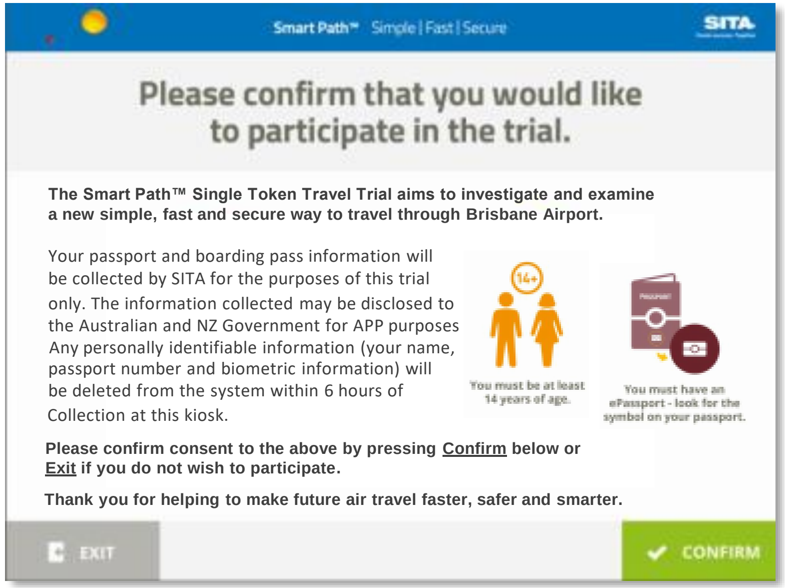
Explicit consent not always necessary !

Definitions

- The data controller, means: the entity which determines the purposes and the means of the processing. In other words: why and how are the data processed?
- The data processor, means: the entity that is processing data on behalf of the data controller; and must follow the instructions given to it by the data controller.
- The data subject, is: the individual whose personal data is being processed (e.g., employee, customer, end-user, vendor/supplier); who can exercise certain rights over his/her data.
- The regulator, is: the national data protection authority that is competent to supervise the data processing operations taking place on its territory; and to enforce compliance with the national data protection law.

Example – Biometric ID Enrolment Screen

Complies with local data privacy requirements



Smart Path™ Simple | Fast | Secure

SITA

Please confirm that you would like to participate in the trial.

The Smart Path™ Single Token Travel Trial aims to investigate and examine a new simple, fast and secure way to travel through Brisbane Airport.

Your passport and boarding pass information will be collected by SITA for the purposes of this trial only. The information collected may be disclosed to the Australian and NZ Government for APP purposes Any personally identifiable information (your name, passport number and biometric information) will be deleted from the system within 6 hours of Collection at this kiosk.

You must be at least 14 years of age.

You must have an ePassport - look for the symbol on your passport.

Please confirm consent to the above by pressing Confirm below or Exit if you do not wish to participate.

Thank you for helping to make future air travel faster, safer and smarter.

EXIT

✓ CONFIRM

"Your face is your boarding pass"

ABOVE. BEYOND.

WHAT IS “PROCESSING” ?

<u>Processing</u> of personal data means:

- Any operation or set of operations which is performed upon personal data, whether or not by automatic means – including:
  - collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction
- <u>Any use of personal data</u> is potentially a processing operation

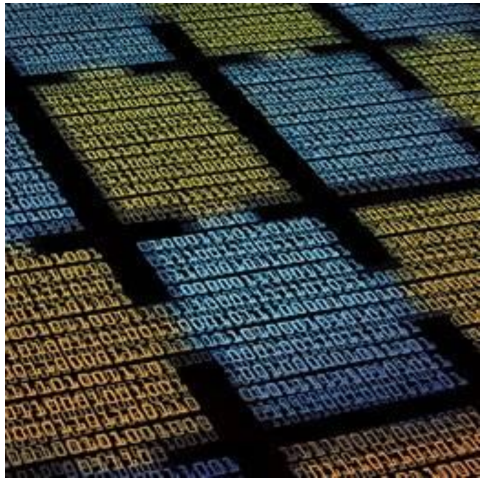
<u>Key requirements</u> – personal data must be:

- processed <u>fairly and lawfully</u> for <u>limited purposes</u> that are <u>adequate, relevant and not excessive</u>;
- <u>accurate</u> and, where necessary, kept up to date;
- kept for <u>no longer than is necessary</u> for the purposes for which the data was collected;
- kept <u>secure and confidential</u>;
- processed in accordance with the <u>restrictions on international transfers</u>.

RIGHTS OF INDIVIDUALS

Individuals have the following rights under GDPR:

- Right to be informed about the collection/processing of their personal data no later than the time of collection
- Right to access and obtain a copy of their data
- Right to amend, correct /update and delete their information
- Right to object to use of their information
- Right to opt-out from / restrict marketing communications
- Right not to be subject to fully automated decisions
- Right to be forgotten



DATA PROTECTION OFFICER (“DPO”)

Role requirements

- Expertise in EU data protection law
- Leadership in data protection management & governance
- Ability to communicate at CEO level
- Sound understanding of IT infrastructure & processes of employer
- Foster a data privacy culture
- Inform, document, advise – including re any data privacy breaches
- Key liaison with (for example):
  - ICO – Information commissioner’s Office (UK)
  - CNIL - Commission nationale de l'informatique et des libertés (France)

QUESTION

- What’s the best prior experience for a DPO: Internal Audit, Legal, Ops, CISO?

THE DPO ROLE – FOCUS ON *PRIVACY GOVERNANCE*

To be efficient, a personal data management organization must conciliate several criteria

Strategical position in the hierarchy	The DPO must have the means to enforce the legislation and be able to bring Privacy stakes to the top management
Independence	The DPO must not be subject to conflict of interest and has the way to act independently from person defining treatments
Legal expertise	The DPO must be able to understand the legislation and its main principles
IS expertize	Most of the treatments lay on applications and IT infrastructures
Integrated into processes	The DPO must identify all new treatments and anticipate non-conformities as soon as possible
Understanding of business activities	The DPO must understand characteristic features of business stakes in order to adapt its actions

Related to the DPO position
(e.g. Define global politic, representation toward senior management)

Related to the DPO associated organization
(e.g. project accompaniment, hold the inventory) …)

Questions
&
Thanks!

Name: Jonas Bartlett
Organisation: SITA
Position: Senior Legal Counsel
Contact: jonas.bartlett@sita.aero

Name: Navdeep Gill
Organisation: SITA
Position: Legal Director
Contact: navdeep.gill@sita.aero