Breakfast Sponsor

Discover Global Network
2018 ATPS APAC SPONSORS
How do you deliver outstanding experiences without inviting fraud?

$858M 1-2% 72%

Cost of payment fraud to the airline industry each year
Of travel agency revenue is used to manage fraud
Of businesses worry about preventing fraud without turning away good customers

sift science
Machine learning can separate fraudsters from real travelers

It's only when you apply behavioral analysis on a large scale, looking at all of a user's activity and all activity of users across the travel industry, that you can get an accurate picture of whether someone is truly who they say they are.

At Sift Science, we have over 16,000 signals we look at to identify fraud. Here are just a few examples:

- Account age
- Time until event
- Seat selection
- Order size
- Destination
- Buyer location
- Device type / ID
- Fare class

Sources: Statista, eMarketer, Zozi, IATA, Phocuswright, Sift Science

To learn more about how Machine Learning can help you prevent fraud email:
Tobias Abdon tobias@siftscience.com

ATPS APAC, Phuket, 2018
GDPR & Regulatory Update
6th September 2018

Kelvin Looi
Global Sales Executive
Unified Governance & Integration
IBM Analytics
Legal Disclaimer

• Notice: Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

• IBM’s statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM’s sole discretion.

• Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

• The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

• The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

• Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user’s job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

None of the statements contained herein constitutes legal advice – it is process advice only.
From May 25th, 2018 

Applies Globally 

to any Organization working with Personal Data of a Data Subject residing in the EU or Profiling From the EU 

4% of Global Revenue or 

€20M Potential Penalty Per-incident 

5 Key General Data Protection Regulation Obligations 

Rights of EU Data Subjects 

Security of Personal Data 

Compliance & Legal Basis 

Accountability of Compliance 

Data Protection by Design and by Default 

Other Regulations 

Singapore PDPA 
Malaysia PDPA 
Japan PDPI Act 
Australia Privacy Act 
Hong Kong PCPD 
California CCPA …
GDPR Key Subjects

Data Subject
(Natural Person)

Personal data means ... an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Controller
(DPO)

... determines the purposes and means of the processing of personal data.

Processor
(DPO)

... processes personal data on behalf of the controller;

(Data Protection Agreement)

(Lawful? Consent?)

(Lawful? Consent?)
Summary by Area:

Rights of EU Data Subjects
- Enhanced rights for data subjects in the EU including notice, access, rectification, erasure, restriction, portability and objection
- Easier access to personal data with more information on processing available both clearly and understandably

Security of Personal Data
- Obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk
- Includes 72H breach reporting to regulatory authorities and without undue delay to individuals in high risk scenarios

Lawfulness and Consent
- Processing only lawful if one of: consent, necessity, legal obligation, protection, public or legitimate interest or official authority
- Consent must be freely given, specific, informed, unambiguous and if a special category or certain other scenarios, explicit

Accountability of Compliance
- Need to demonstrate compliance with the principles relating to personal data processing pervades throughout the GDPR
- Include lawfulness, fairness, transparency, purpose/storage limitation, minimisation, accuracy, integrity and confidentiality

Data Protection By Design and By Default
- Data controllers must implement technical and organisational measures demonstrating compliance with GDPR core principles
- Ensure the rights of data subjects are met and that only data necessary to the specific purpose are processed
Article 5: **Principles relating to personal data processing**

1. Personal data shall be:
   a) processed lawfully, fairly and in a transparent manner …
   b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes …
   c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
   d) accurate and, where necessary, kept up to date; …
   e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; …
   f) processed in a manner that ensures appropriate security of the personal data,…

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6: **Lawfulness of processing (... is necessary,... given consent, …)**
Article 7: **Conditions for consent**
Article 8: **Conditions applicable to child's consent in relation to information society services**
Article 13: Information to be provided where personal data are collected from the data subject
Article 14: Information to be provided where personal data have not been obtained from the data subject

Article 15: Right of access by the data subject
Article 16: Right to rectification
Article 17: Right to erasure ('right to be forgotten')
Article 18: Right to restriction of processing
Article 20: Right to data portability
Article 21: Right to object

Article 25: Data protection by design and by default
Article 30: Records of processing activities
Article 32: Security of processing

Article 33: Notification of a personal data breach to the supervisory authority ('...the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it.)
Article 34: Communication of a personal data breach to the data subject ('... the controller shall communicate the personal data breach to the data subject without undue delay')
IBM has established a global readiness program tasked with identifying the key impacts of the GDPR across IBM’s business and preparing IBM’s internal processes and commercial offerings for compliance with the GDPR.

The programme is organised into several work streams, staffed with IBM’s top data privacy and security professionals. Focal points in each Business Unit are responsible for implementing the GDPR-related policy, system and business process changes mandated by the various key work streams.
IBM’s Overall GDPR Framework: 5 Phases to Readiness

**Assess**
- Conduct GDPR risk & privacy assessments across governance, people, processes, data, security
- Develop GDPR Readiness Roadmap
- Identify & Map personal data

**Design**
- Design governance, training, communication, and process standards
- Design privacy, data management and security management standards

**Transform**
- Develop and embed procedures, processes and tools
- Deliver GDPR training
- Develop & embed standards & policies using Privacy by Design, Security by Design
- Detailed Data Discovery

**Operate**
- Execute all relevant business processes
- Monitor security and privacy using TOMs
- Manage Consent & data subject access rights

**Conform**
- Monitor, assess, audit, report and evaluate adherence to GDPR standards

**Outcome**
- Assessments and roadmap
- Defined implementation plan
- Process enhancements completed
- Operational framework in place
- Ongoing monitoring and reporting

Identify GDPR impact and plan Technical and Organisational Measures (TOM)
Includes Data Protection controls, processes and solutions to be implemented
TOMs in place: Personal Data discovery, classification and governance in place
Begin the new GDPR ready way of working
Monitor TOMs execution; deliver compliance evidence to internal and external stakeholders

ATPS APAC, Phuket, 2018
5 Key Data Governance Areas to Get Ready for GDPR

Which one to start with depends on where you are today

1. **Discovery and Mapping**
   - Know your relevant data: Understand where personal data resides

2. **Records of Processing Activities (Art. 30)**
   - Capture your processing activities on personal data and demonstrate progression towards Article 30 readiness

3. **Access by the Data Subject**
   - Enable your organization to respond to access requests by Data Subjects within the timescales defined in GDPR

4. **Governance and Lifecycle Management**
   - Protect Personal Data: Safeguard data by applying anonymization and minimization techniques

5. **Manage Consent**
   - Help you manage consent of Data Subjects to meet the GDPR standard

---

**Analytics Building Block Journey**

Which one to start with depends on where you are today.
Are You Ready for GDPR?

Pre-Travel
- Travel Plan
- Travel Agent
- Loyalty Program
- Airline Agent
- Purchase
- Call Center

Travel
- Check-in
- Lounge
- Merchandise Purchase
- Board
- Wi-fi
- Entertainment
- Luggage Claim
- Lost & Found
- Arrival Service

Post-Travel
- Survey
- Campaign
- GDPR Request

GDPR Ready?

Supporting Systems
- Web
- Mobile
- Loyalty
- Reservation
- Call Center
- Travel Agent
- Airline Agent
- Pre-flight Operation
- Lounge
- Merchandise
- In-flight Operation
- Claims
- Survey
- Business Intelligence
- Campaign

Article 13: Information to be provided where personal data are collected from the data subject

Article 14: Information to be provided where personal data have not been obtained from the data subject

Article 15: Right of access by the data subject

Article 16: Right to rectification

Article 17: Right to erasure ('right to be forgotten')

Article 18: Right to restriction of processing

Article 20: Right to data portability

Article 21: Right to object

ATPS APAC, Phuket, 2018
Are You Ready for GDPR?

On July 17, 2018, the Dutch Supervisory Authority announced that it will start a preliminary investigation to assess whether certain large corporations comply with the EU's General Data Protection Regulation ("GDPR") – see the official press release [here](https://example.com) (in Dutch). To that end, the authority will review the “records of processing activities” from thirty randomly selected corporations which are located in the Netherlands. … Source: The National Law

European data protection bodies have promised to work closely with their Irish colleagues on multi-billion-euro complaints filed by Austrian privacy campaigner [Max Schrems](https://example.com) against [Facebook](https://example.com) and [Google](https://example.com). … Source: The Irish Times

May 25, 2018

The implementation of the General Data Protection Regulation (GDPR) across the EU last May has had quite an impact on the Danish Data Protection Agency (DDPA). The agency has seen a tremendous spike in cases being processed and expects to have to handle 20,000 cases this year – a quadrupling of the average 5,000 cases it usually processes annually…. Source: CPH Post Online Aug 20, 2018
Thank You