A Comparison of GDPR Compliance Evaluation Methods

I. DEVELOP PROCESS MODEL
- Contact center of major European Airline
- Flight booking process selected

II. GDPR COMPLIANCE EVALUATION
- Focused on consent, data security, transparency and processing activities
- Relevant articles (5, 6, 7, 13, 24, 26) were instantiated in terms of business process model
- New compliance identified

III. PROCESS CORRECTION
- Non-compliance addressed
- New activities introduced
- GDPR assessment tables created
- Validate the introduction of new activities in addressing non-compliance
- New flight booking process modeled

IV. VALIDATION
- Each new activity further modeled at subprocess level
- New processes and subprocesses validated by experts at the airline through interviews.

FLIGHT BOOKING PROCESS

GDPR COMPLIANCE CHECKING

I. EXTRACT AS-IS COMPLIANCE MODEL:
- Use set of predefined extraction rules
- Extract: GDPR Meta-model, Business Process in BPMN notation, Business Processes centered (addition)
- Input: GDPR Meta-model, Business Processes centered

II. COMPARE TWO MODELS:
- Extract: GDPR Meta-model and As-is compliance model
- Output: Differences in two models
- Missing classes? Change Attributes?
- Constraints are passing?

III. DEFINE COMPLIANCE ISSUES:
- Highlight compliance issues based on comparison of two models
- Input: Differences in two models
- Output: Compliance issues

IV. CHANGE BUSINESS PROCESS
- Rectify business process to meet requirements highlighted in previous step
- Input: Compliance issues
- Output: Business Process

INTERVIEW PROCESS

Interview setup
- Face to face
- 45-60 minutes
- Brief presentation followed by discussion
- All interviews conducted within one week

Provided materials
- Summary of GDPR articles
- The flight booking process (To-Be)
- Questions

Analysis method
- Rhetorical approach was used
- Close-ended questions
- Results classified manually under each key area in p. 20

RESULTS

81% STRONG CORRESPONDENCE

UNIQUE RESULTS
- Lack of secure payment system (Appropriate technical safeguards Article 24)
- Lack of transparency (Article 5)

SIMILAR RESULTS
- Implementation of consent activity
- Communicate purpose of data processing (Sending privacy notice)
- Rights to rectification and access

UNIQUE RESULTS
- Data processing activities were not logged [Art. 39 GDPR]
- Implementation of all processes to fulfill data subject’s rights [Art. 15-20 GDPR]