Lufthansa Industry Solutions

myIDTravel and myDutyTrip

Data Protection Measures

pursuant to Article 28 General Data Protection Regulation (GDPR), valid from May 25th, 2018

Version 4.2
Date 13.03.2020

Lufthansa Industry Solutions

Statement of Confidentiality

The information in this document is the property of Lufthansa Systems Business Solutions GmbH hereafter referred to as Lufthansa Industry Solutions. Lufthansa Industry Solutions submits this document with the understanding that it will be held in strictest confidence and will not be disclosed, duplicated or used, in whole or in part, for any purpose other than the evaluation of the qualifications of Lufthansa Industry Solutions, without prior written consent.

Version	Date	Author	Revision Notes	Status
1.0	17.09.2010	[redacted]	First Version	completed

2.0	24.11.2015	[redacted]	Revision	completed
2.1	21.02.2018	[redacted]	Revision acc. GDPR	draft
3.0	04.04.2018	[redacted]	Completion acc. GDPR	completed
4.0	11.04.2018	[redacted]	Revision	completed
4.1	24.05.2018	[redacted]	Review and Approval acc. GDPR	final
4.2	13.03.2020	[redacted]	Revision	final

Contents

1 Data protection of personal data processed with myIDTravel or myDutyTrip

All personal data used in myIDTravel or myDutyTrip are being processed by

- Lufthansa Industry Solutions BS GmbH
- Lufthansa Industry Solutions AS GmbH
- Lufthansa Industry Solutions TS GmbH
- Lufthansa Systems Poland
- Lufthansa Systems Hungaria
- Lufthansa Industry Solutions Shpk, Albania
- IBM Deutschland Aviation Industry Services GmbH

collectively called the “Data Processors” at

- the Lufthansa Industry Solutions BS GmbH premises in Raunheim, Germany
- the Lufthansa Industry Solutions AS GmbH premises in Raunheim, Germany
- the Lufthansa Industry Solutions TS GmbH premises in Oldenburg, Germany
- the Lufthansa Industry Solutions Lufthansa Industry Solutions Shpk, Albania
- the Lufthansa Systems Poland premises in Gdansk, Poland
- the Lufthansa Systems Hungaria premises in Budapest, Hungary
- IBM Deutschland Aviation Industry Services GmbH, Frankfurt/Main, data center in

Kelsterbach, Germany.

In order to protect the personal data, the Data Processors fully complies with the requirements of the European General Data Protection Regulation in force from 25th May 2018.

Based on the obligations set forth in the above mentioned General Data Protection Regulation (hereinafter referred to as "GDPR"), the Data Processors have set up the following measures:

- processing the personal data only on behalf of the client and in compliance with GDPR,
- implementation of technical and organisational security measures specified in section 2 before processing the personal data transferred.

2 Data protection measures effective for myIDTravel and myDutyTrip

Description of the technical and organisational security measures implemented by the Data Processors in accordance with GDPR:

2.1 Pseudonymization and encryption of personal data (Art. 32 para. 1(a) of the GDPR)

Pseudonymization

Processing personal data in a manner such that personal data can no longer be attributed to any specific data subject without consulting additional information, provided that this additional information is kept in a separate location and is subject to technical and organizational measures.

Description of measures taken:

- Pseudonymization of activity logs except where storage is required for operational or legal reasons

Encryption

Use of procedures and algorithms that convert personal data into non-readable form by using digital or electronic codes or keys. Symmetric and asymmetric encryption technologies may be used.

Description of measures taken:

- 2-way SSL
- message encryption
- file transfer via sftp

2.2 Measures to ensure confidentiality (Art. 32 para. 1 (b) of the GDPR)

Physical access control

Technical and organizational measures for physical access control including, without limitation, identification of authorized persons.

Description of measures taken:

- access control system, ID card readers
- door security (electrical door openers)
- site security, concierge
- surveillance facilities for alarm systems, video/TV monitors
- multi-layer access controls

System access control

Technical measures (keyword/password protection) and organizational measures (master user data set) for user identification and authentication.

Description of measures taken:

- password policy (incl. special characters, min. length, regular renewal)
- automatic lock-out (e.g. password or logout on breaks)
- set up of a use master data record per user

Data access control

Access authorization and data access rights granted on need-to-know basis, as well as monitoring and tracking access.

Description of measures taken:

- graded authorization model (profiles, roles, transactions, objects)

Separation control

Measures to ensure separate processing (storage, modification, erasure, transmission) of data serving different purposes.

Description of measures taken:

- internally multi-client enabled / limitation of use for a specific purpose
- functional separation (live, test)

2.3 Measures to ensure integrity (Art. 32 para. 1 (b) of the GDPR)

Transfer control

Measures for migration, transfer, transmission or storage of data to or on data carriers (manually or electronically), and measures for subsequent review.

Description of measures taken:

- encryption
- electronic signatures (e.g. for Single-Sign-On and Staff Profile Upload Service and e-mails)
- logging
- transport security

Input control

Measures for documentation of data administration and maintenance as well as subsequent review whether and by whom data were input, modified, or removed (erased).

Description of measures taken:

- systems for logging and for log file analysis

2.4 Availability and resilience of systems and services (Art. 32 (b) of the GDPR)

Availability control

Measures for (physical/logical) data backup, so that data is protected against accidental deletion or loss.

Description of measures taken:

- back-up procedures
- hard drive mirroring, e.g. RAID method
- uninterruptible power supply (UPS)
- archive storage in 2 different data center slides
- virus protection, firewall
- emergency plan

Availability of IT systems used

Description of measures taken:

- back-up procedures
- redundant application servers, database servers and PCI servers
- hard drive mirroring
- uninterruptible power supply
- redundant internet connectivity
- virus protection
- firewalls
- emergency plan

2.5 Measures to restore availability and access to personal data in the event of a technical incident (Art. 32 (c) of the GDPR)

Recovery/backup systems

Description of measures taken:

- daily incremental backup and weekly full backup
- regular database replication

2.6 Procedures for the regular review, assessment, and evaluation of technical and organizational measures (Art. 32 para. 1 (d) of the GDPR; Art. 25 para. 1 of the GDPR)

Data protection management

Description of measures taken:

- Repeated external and internal audits
- Inspection of infrastructure is done according to defined maintenance schedules

Data protection-friendly default settings (privacy by default)

Description of measures taken:

- Repeated external and internal audits
- Inspection of infrastructure is done according to defined maintenance schedules

Contract control

(Technical/organizational) measures to define the respective competencies of the Data Processors for the assurance of policy-compliant processing of contractual data.

Description of measures taken:

- unambiguous contract drafting
- formal contract awarding process (contract form)
- criteria for selecting contractor

- monitoring of contractual fulfilment