ACCEPT Institute

Horizon 2020 ETC 636126

Smart Privacy Requirements / Audit Procedures

–

Deliverables D4.2 & D4.3

08 December 2017

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 636126.

1 Introduction

1.1 Introduction

This document is both Deliverable 4.2 and Deliverable 4.3 and is part of work package 4 '*Define & Plan for the Traveller-in-Control Privacy Solutions*'.

The goal of the Privacy Solution of the European Travellers Club (ETC) is to maintain a relation based upon long-term trust from both its travellers as its traveller organisations. In Deliverable 4.1 Privacy Reference Design a detail of the goal was presented, towards the creation of a *Reference Design* that should be included in the implementation of the core systems of the ETC and its members. Deliverables 4.2 and 4.3 follow this deliverable towards Requirements (or Regulations) and Procedures to audit these.

The Requirements are also in accordance with the new General Data Protection Regulation (GDPR).

These Requirements, or regulations are examples of the clauses that are included in ACCEPT Franchise Agreements (see also deliverable 3.6) between parties pertaining to the use of personal data.

With the finalisation of Deliverable 4.2 and 4.3 the Deliverable 4.1 now has reached the status of final as well.

2 Content

1 Introduction 2
1.1 Introduction 2
2 Content 3
3 Smart Privacy Requirements / Audit Procedures 4
4 Chapter 1 - General Provisions 5
5 Chapter 2 - General Requirements 8
6 Chapter 3 - Planning 9
7 Chapter 4 - Execution and Implementation 11
8 Chapter 5 - Training 14
9 Chapter 6 - Handling Complaints 15
10 Chapter 7 - Inspection 16
11 Chapter 8 - Reviews 17
12 Chapter 9 - Penalties 18
13 Chapter 10 - Revision or Repeal 19

3 Smart Privacy Requirements / Audit Procedures

Below the Smart Privacy Requirements or regulations for the ETC-system are presented. These requirements, or regulations are examples of the clauses that should be included in ETC agreements between parties pertaining to the use of personal data.

This is relevant for all ETC-systems and ETC-members.

4 Chapter 1 - General Provisions

Article 1. Objective

These Regulations have the objective of properly protecting personal data collected through the ETC-system operated by ACCEPT Institute, and thus protecting individuals' rights.

Article 2. Scope

These Regulations shall apply to units collecting, using or storing personal data through the ETC-system operated by ACCEPT Institute.

Article 3. Duty of Compliance

All persons who collect, use and store personal data through the ETC-system operated by ACCEPT Institute shall comply with these Regulations. Employees of subcontractors shall be required to comply with these Regulations through the subcontractor to which they belong.

Article 4. Definitions

1. Personal Data

   Any information relating to an identified or identifiable person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity[1].

[1] *Quoted from the Directive 95/46/EC of the European Parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*

2. Processing of personal data

Any operation or set of operations which is performed upon personal data, whether or not by automatic means.

3. Data subject

The particular individual identified by the personal data.

4. The data subject's consent

Any indication of the data subject's wishes by which he or she explicitly approves, whether in writing or by other means, the processing of personal data relating to himself or herself, after being informed about the collection use or provision of personal data.

5. Third Party

Any party other than the data subject or the organization processing the personal data.

6. Notify

To inform the data subject directly by post, telephone, electronic mail or other means.

7. Contact the data subject

To communicate with or contact the data subject by post, telephone, electronic mail or other means.

8. Disclosable personal data

A set of information organized systematically so that it can be searched using a computer, or a set of information organized systematically to facilitate retrieval of specific personal data by systematizing, classifying or analyzing it in accordance with certain rules and attaching a table of contents, an index of markings, which

information ACCEPT Institute is fully authorized to disclose, correct, supplement, or delete, cease using, erase or cease providing to a third party at the request of the data subject.

9. Processor of personal data

Any person who collects, uses, stores, or otherwise handles personal data, including any person specified in article 9 of these Regulations.

10. Automated Processing

Automatically processing personal data according to certain criteria: for example, deducing personal preferences and characteristics by analyzing camera usage history or customer purchase history.

Article 5. Legal Compliance

When collecting, using or storing personal data, relevant domestic and foreign laws, including those of the EU, shall be considered and obeyed. The relevant EU laws shall be fully followed especially when personal data is transferred outside the EU with its respect for protection of privacy and for individuals' rights. It shall be kept in mind that data subjects can sue ACCEPT Institute for damages if a legal violation adversely affects them.

Article 6. Working with Personal Data

Personal data shall as a rule be recorded in fixed, tangible form on paper or a photographic medium, on an electronic or magnetic medium or by other means, and displayed in a format that can be viewed either directly or using a device (which format is referred to below as a "document"); and anyone working with the data shall do so using that document. This does not apply, however, to data that by their nature are not conducive to documentation, or to data concerning minor matters.

5 Chapter 2 - General Requirements

Article 7. Compliance with the Privacy Protection Policy

Any unit collecting, using or storing personal data through the ETC-system operated by ACCEPT Institute shall do so in full accordance with the ACCEPT Institute Privacy Protection Policy formulated and internally and externally released by ACCEPT Institute.

6 Chapter 3 - Planning

Article 8. Specifically Identifying personal Data Collected

Processors of personal data shall specifically identify the personal data collected through the ETC-system operated by ACCEPT Institute and compile a personal data management sheet including the retention period. The personal data processing supervisor shall check the contents of the management sheet as necessary and endeavor to keep it up to date.

Article 9. Functions, Responsibilities and powers

1. The head of any unit collecting, using or storing personal data through the ETC-system operated by ACCEPT Institute shall, as the person ultimately responsible for protection of those personal data, have responsibility and authority for formulating, executing and improving policies and plans for securely protecting personal data.
2. The personal data protection manager shall have responsibility and authority for managing procedures for securely protecting personal data collected through the ETC-system operated by ACCEPT Institute.
3. The personal data protection audit supervisor shall have responsibility and authority for auditing and reporting.
4. Auditors, appointed by the personal data protection audit supervisor, shall have responsibility and authority for conducting audits.
5. The personal data processing supervisor shall have responsibility and authority for managing personal data in any unit processing personal data obtained through the ETC-system operated by ACCEPT Institute.
6. Personal data processing staff shall have responsibility and authority for properly collecting, using and storing personal data through the ETC-system operated by ACCEPT Institute.

Article 10. Written Plans

1. The personal data protection manager shall formulate and execute the training plans necessary to securely protecting personal data.

2. The personal data protection audit supervisor shall formulate and execute audit plans for verifying that personal data are securely protected.

Article 11. Preparation for Emergencies

1. Upon discovering that an incident involving personal data, such as loss, disappearance, theft, tampering, destruction, leakage or unauthorized use, has occurred or could occur, any person defined in Article 3.1 as having a duty to comply with the Regulations shall immediately inform the following persons:

    a. The personal data processing supervisor responsible for the personal data in question; and

    b. The personal data protection manager.

2. Upon being so informed, the personal data processing supervisor and the personal data protection manager shall immediately ascertain the facts of the case and expeditiously implement the necessary measures such as taking steps to minimize the impact. Depending on the extend of the impact, their findings shall be reported internally and if necessary additional instructions shall be obtained on how to proceed.

7 Chapter 4 - Execution and Implementation

Article 12. Principles Governing Collection, use and Provision of Data

1. Specifying the Intended Use
   Recipients of personal data shall specify the intended use for which the data are being collected and shall collect, use and store those data only to the minimum extend necessary for that purpose. If necessary under the legal system of the country in question, they shall also file notice of the use of the personal data with a data protection authority or other relevant body. Further, they shall explicitly obtain the consent of the data subject when collecting the data, including if the intended use has changed, and shall clearly identify the data acquisition source.

2. Appropriate Collection of Data
   Recipients of personal data shall collect personal data by legal, fair means.

3. Procedures for using data
   Users of personal data shall use those data only insofar as necessary for the specified intended use and in a way not detrimental to the data subject.

4. Procedures When Contacting the Data Subject
   Users of personal data shall, if contacting a data subject beyond what is necessary for the intended use of the personal data collected, notify the data subject of the intended use, method of collection etc., and obtain his or her consent. They shall also notify the data subject if accessing personal data for automated processing.

5. Procedures for Provision of Data
   Except if otherwise provided for by law or regulations, processors of personal data shall, when providing personal data collected to a third party, first notify the data subject of the purpose for which the data are to be provided to the third party and who the recipient is, and obtain his or her consent.

Article 13. Proper Management of Data

1. Ensuring Accuracy
   Processors of personal data shall keep those data as accurate and up to date as necessary for their intended use. They shall also regularly check whether the

personal data need to be updated. Further, they shall completely erase any personal data that are no longer needed.

2. Security Management Procedures
   The following persons shall, depending on the risks associated with the personal data being processed, take the necessary and appropriate steps to prevent the data from being leaked, lost or damaged and to otherwise manage the security thereof:

   a. Personal data processing staff;

   b. The personal data processing supervisor; and

   c. The personal data protection manager

3. Supervision of Employees
   The personal data processing supervisor and the personal data protection manager shall appropriately supervise personal data processing staff as necessary to ensure that personal data are securely managed.

4. Supervision of Subcontractors

   The following persons shall, when the processing of personal data is outsourced in whole or in part, select a subcontractor that takes measures to protect personal data at least as rigorous as ACCEPT Institute, and shall conclude a suitable contract with it. They shall also appropriately supervise the subcontractor as necessary to ensure that personal data are securely managed.

   a. Personal data processing staff;

   b. The personal data processing supervisor; and

   c. The personal data protection manager

Article 14. Rights of Data Subjects with Respect to Personal Data

1. Rights with Respect to Personal Data

   In case of a request for verbal or written disclosure etc. from a data subject who has provided personal data, personal data processing staff shall, after verifying the person's identity, respond promptly and appropriately in accordance with the law.

2. Procedures for Responding to Disclosure and Other Requests

Personal data processing staff shall establish an organizational framework and procedures for responding to disclosure and other requests, and shall ensure that these are readily ascertainable by data subject.

3. Correcting, Supplementing or Deleting Disclosable personal Data

   If requested, either by the data subject or by a court, to correct, supplement or delete disclosable personal data by which the data subject can be identified on other grounds that for example the information is false, personal data processing staff shall conduct the necessary investigation without delay insofar as necessary for making the correction as such. Unless special procedures are prescribed by law, the disclosable personal data shall be corrected, supplemented or deleted on the basis of the results thereof.

8 Chapter 5 - Training

Article 15. Training in Personal Data Protection

Processors of personal data shall receive training in protection of personal data, including these Regulations regularly or as necessary.

9 Chapter 6 - Handling Complaints

Article 16. Responding to Complaints and Inquiries

Personal data processing staff shall respond promptly and appropriately to complaints and inquiries from data subjects about processing and protection of personal data.

10Chapter 7 - Inspection

Article 17. Verifying Implementation

Personal data processing staff and personal data processing supervisors shall regularly verify that personal data are duly protected.

Article 18. Auditing

Auditors and personal data protection audit supervisors shall regularly audit the state of personal data management. The audit findings shall be reported to ACCEPT Institute.

11Chapter 8 - Reviews

Article 19. Reviews

In order to comply with laws, regulations and guidelines, the heads of units collecting, using of storing personal data through the ETC system operated by ACCEPT Institute shall regularly review policies on and the organizational framework and technical measures for protecting personal data, taking into account changes in internal and external environment.

12Chapter 9 - Penalties

Article 20. Penalties for Violations

Violations of these Regulations shall be dealt with as prescribed in the ETC member agreements.

13 Chapter 10 - Revision or Repeal

Article 21. Revision or Repeal

Revisions to or repeal of the Regulations shall be proposed by a personal data protection manager and decided by the head of the unit collecting, using or storing personal data through the ETC-system operated by ACCEPT Institute.