Katso Identification System

1. Controller
Population Register Centre
P.O.Box 123 (Lintulahdenkuja 4 A)
FI-00531 Helsinki
telephone +358 295 535 001
fax +358 9 876 4369
kirjaamo[at]vrk.fi (registry office)

2. Information concerning the register or personal data file
Electronic filing support services, Information Systems Manager Petteri Kivimäki
firstname.lastname[at]vrk.fi
tel. 0295 535 027.

3. Name of register or personal data file
Katso Identification System (Katso-tunnistuspalvelu).

4. Purpose of processing personal data (purpose of use of the register)
Online recognition and authorization management of corporate taxpayers and organizations, and the physical persons representing them are the purposes of the system.
During its online processes the system captures and saves the user data listed below under "(6) Information content of the captured data in the personal data file".

5. Groups of system-registered users
Representatives of the organization concerned, staff members of the public office handling the registration of customers.

6. Information content of the captured data in the personal data file
For customers:
• Personal ID number
• Name and address
• e-mail
• Sign-in identifier (User ID)
• Timestamp
• Method of online recognition
• If online recognition failed, facts about the failure
• Consent of Data Subject for system-based handling of personal data.

For staff members:
• Name
• Timestamp.

The customer accepts the Katso Terms and Conditions to give consent and acceptance for having the Katso system handle the customer's personal data.

7. Regular Sources of Data in the File
The databases of The Population Register Centre´s customer register, Trade Register, Register of Associations and Foundations.

8. Specification of regular destinations of disclosed data and whether data are transferred to countries outside the European Union or the European Economic Area
The personal identity code or a comparable identifier of a Data Subject, and/or a User ID enabling him or her to sign in can with the Data Subject's consent be transferred to the public authorities that either use the sign-in service or perform other public duties.

9. Description of the principles in accordance to which the data file has been secured
The Katso network and the hardware in which the Katso data file is stored are firewall protected. All information interchange relating to personal data is secured. Furthermore, the data records are protected against unauthorized viewing, editing and deletion. This protection is based on physical access control, User IDs and limitations of user privileges. User privileges for viewing and editing are restricted according to the job descriptions of the staff, and all viewing and editing sessions are logged. Data integrity is secured by means of automatic and manual error checks during several data processing stages. Backup procedures and physical safety measures protect the data against accidental erasure. Paper printouts relating to the contents of the data file are protected by access control and appropriate archiving arrangements.

10. Right of access
The data subjects have no right of access to their data.

11. Right to request the correction of data
No right to request correction of data.

12. Other rights related to the processing of personal data
The data subjects have no other rights related to the processing of personal data.