EuroPriSe
European
Privacy Seal

European Privacy Seal
– *privacy at its best*

HUAWEI ID
(core functionalities)
as provided by Aspiegel SE
to users in the EU/EEA
Short Report

Version History

Version	Date	Reason for Changes	Author(s)
1.0	08-12-2023	Initial Version	Arghya Biswas
1.1	13-12-2023	Feedback by review team	Sebastian Meissner

Table of Contents

List of Figures

1. Type of Certification and Applicable EuroPriSe Specification Documents

Type of Certification
Processing operations by a controller (controller service)
Initial certification (under the new EuroPriSe procedure)

Applicable Criteria Catalogue
EuroPriSe criteria for the certification of IT products and IT-based services v201701

Applicable Rules of Procedure
EuroPriSe rules of procedure v2.0

Applicable Evaluation Compendium
EuroPriSe compendium of evaluation methodology v2.0

Applicable Matrix of Evaluation Methods
Matrix evaluation types and methods v2.0

2. Name of the Certification Customer and General Information about Them

Name of the Certification Customer
Aspiegel SE

Address of the Certification Customer
3rd floor, Mespil Court
Mespil Road, Ballsbridge
Dublin 4, D04 E516, Ireland

Membership of a Group of Companies
Aspiegel SE is a wholly owned subsidiary of HUAWEI Group.

Sector in Which Certification Customer Primarily Operates
Consumer Services, Information Technology

3. Information on the Target of Evaluation ("ToE Description")

Name of the ToE

HUAWEI ID (core functionalities) as provided to users in the EU/EEA

Description of the ToE in Plain Text

Aspiegel SE is a digital service provider headquartered in Dublin, organized and existing under the laws of Ireland, it is governed by Irish Law and supervised by the concerned Irish regulatory authorities. In particular, Aspiegel SE's data processing activities are governed by Irish data protection law and supervised by the Office of the Irish Data Protection Commissioner. Aspiegel SE is a wholly owned subsidiary of HUAWEI Group.

Aspiegel SE offers a variety of mobile services to their customers. HUAWEI ID is a central service, which can be used to log in to other services ("HUAWEI Mobile Services"), such as AppGallery, Mobile Cloud, Developer Alliance, Video, Browser, Assistant, Music, Themes, etc. as well as to (3rd party) apps.

An overview of these services is provided to the user while creating the HUAWEI ID. This is shown in the figure below:

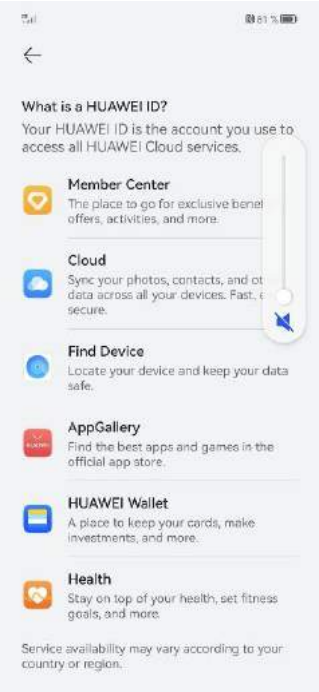

Fig 1: Overview of Services Accessible via Huawei ID

To create a HUAWEI ID, the user needs to provide the following personal information during the registration process.

- Country code;

- E-Mail for registration using E-Mail;
- Phone Number for registration using Phone;
- One-Time password received on E-Mail or Mobile for the respective method;
- Date of Birth.

Core functionalities of the HUAWEI ID are registration (with e-mail address / phone number), login / logout, account modification, account deletion, child account, privacy center, and request a data copy.

The registration process via E-Mail and Phone Number can be seen in the following figures:

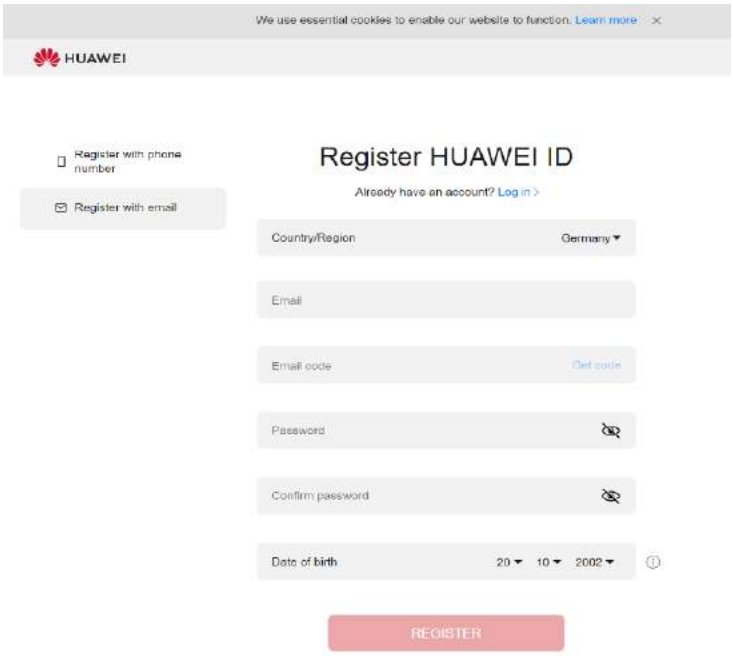

Fig 2: HUAWEI ID Registration using E-Mail

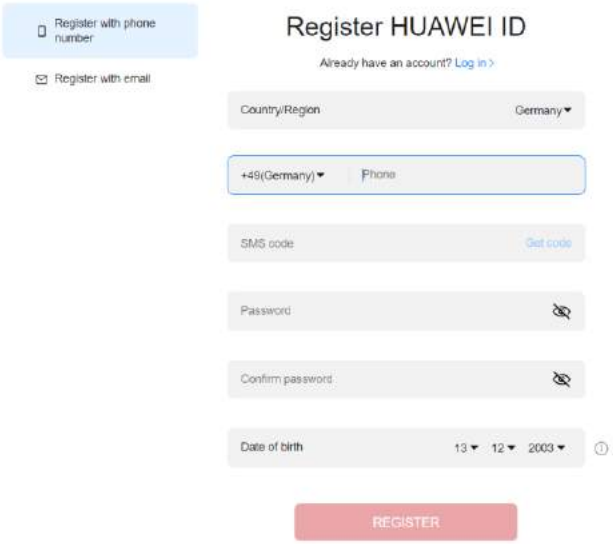

Fig 3: HUAWEI ID registration using Phone Number

Two factor authentication for the registration and 'captcha verficiation' are shown below:

Fig 4: 2-Factor Authentication for Registration

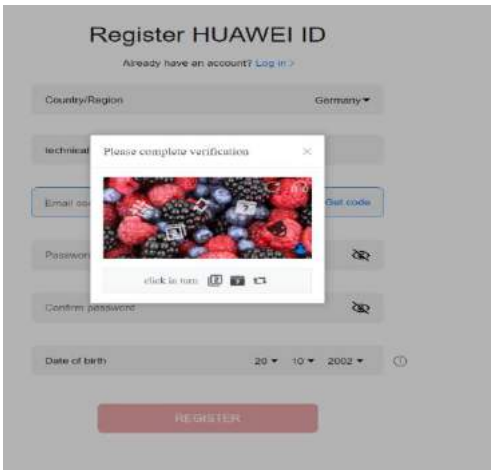

Fig 5: Captcha Verification

The ToE of this certification are the core functionalities of HUAWEI ID as provided to users in the European Union (EU)/European Economic Area (EEA). Other mobile services or apps provided by Aspiegel SE or any 3rd parties do not form part of this target of evaluation. Furthermore, disclosure of data from the HUAWEI ID service to other services or 3rd party service providers is not part of ToE. In other words: The 1st party single sign-on (SSO) process was examined as part of the evaluation and is as such covered by the certification. However, the actual use of the ToE in connection with a dedicated service is not covered by the certification.

Data processed with HUAWEI ID is stored and processed in data centres in Germany. Despite of this, a transfer of personal data to third countries is inherent to the ToE, as is explained in the following: Due to the fact that HUAWEI ID is a global service, there needs to be a way to ensure that users cannot create an account with the same credentials (i.e. under the same email or phone number) on a global level twice. In order to ensure global uniqueness of the account, strictly limited information (a unique

ID as well as the hashed email address and phone number of the user) is synchronised across different sites providing HUAWEI ID accounts. Globally, HUAWEI ID is provided by three different entities, Aspiegel SE being one of them. The other entities (processors) are located in Hong Kong and China. They make use of sub-processors located in further third countries (a list of all third countries concerned is provided below at “Transfer(s) to 3rd Countries”). The unique ID as well as the hashed email address and the hashed phone number qualify as pseudonymised personal data. The hashing (SHA-256 algorithm) is done in a non-reversible way. Together with standard contractual clauses, this hashing (as a supplementary measure) legitimises the transfers to third countries inherent to the ToE (as will be further explained below in this short report).

Specification of Essential Aspects of the ToE

Processing Operations, Processes & Functionalities

To create a HUAWEI ID, the user needs to provide the following personal information during the registration process.

- Country code;
- E-Mail for registration using E-Mail;
- Phone Number for registration using Phone;
- One-Time password received on E-Mail or Mobile for the respective method;
- Date of Birth.

Core functionalities are registration (via phone number and email verification), login/logout, account modification, account deletion, child account, set up emergency contact.

Purpose(s)

Provide HUAWEI ID service and fulfil the contractual obligations, including creation and use of HUAWEI ID, customer support and communication, maintenance, problem diagnosis and fixing. User can login with his/her HUAWEI ID to access HUAWEI Mobile Services such as Mobile Cloud, AppGallery, Video, Music, Themes and more. Personal data are also processed for marketing, business development and IT security purposes.

Categories of Data Subjects

Consumers who use HUAWEI Mobile Services in the European Union (EU)/European Economic Area (EEA). This includes minors.

Categories of Personal Data

Personal data provided directly by data subjects:

- Email address;

- Security email address;
- Phone number;
- Security phone number;
- Registration country (to determine contractual country);
- Name (first and last name);
- Date of birth (date/month/year) (to identify minors);
- Emergency contacts' phone number and name (optional);
- Password;
- Account identifier;
- Profile picture;
- Nickname;
- Gender;
- QR code login information;
- Automatic SMS code information;
- Log Data (types: server system operation, database backup, system access, end user activity, device side application);
- Security events (e.g. password changes, account deletions, app authorization cancellations, account freezing, and indications that an account is at risk of being hijacked);
- User agreement information.

Relevant Locations

Offices of the certification customer: Headquarters are in EU /EEA (Ireland).
Data centres operated by T-Systems International GmbH (EU / EEA).

Transfer(s) to 3rd Countries

A unique ID as well as the hashed e-mail address and phone number of the user is transferred to China, Hong Kong, Malaysia, Russia, and Singapore for uniqueness verification of HUAWEI ID.

Area of Application

HUAWEI ID is used by consumers (mobile service users) in the European Union (EU)/European Economic Area (EEA) in order for them to register an account, modify account information, login to other mobile services, etc.

Processing Operations forming part of the ToE

The Target of Evaluation (ToE) includes:

- HUAWEI ID client on smartphone;
- HUAWEI ID web portal (https://id7.cloud.huawei.com/CAS/portal/login.html);
- The core functionalities are registration (via phone number and email verification), login/logout, account modification, account deletion, child account, set up emergency contact;

- All processes and interfaces related to the processing of personal data of users for direct marketing and business development purposes to the extent it is directly related to the ToE as such;
- 1st party single sign-on service as it is provided by Aspiegel SE (part of HUAWEI ID login (UUID));
- Data transfer / synced (hashed email and/or phone number) to China, Hong Kong, Malaysia, Russia, and Singapore for uniqueness verification of HUAWEI ID.

Processing operations not part of the ToE

The ToE does not include:

- Other HUAWEI mobile services provided by Aspiegel SE or any of their affiliates or any 3rd parties;
- Data disclosure from HUAWEI ID to other HUAWEI mobile services / 3rd party services as well as (3rd party) apps that may interact with the ToE;
- Functionalities / services
  - Facial / Fingerprint authorization;
  - Find my phone;
  - Payment functionalities including the (optional) storage of credit card data in the HUAWEI ID account;
  - My addresses;
  - Friends and contact services;
  - Ads personalization;
  - Check of profile for hateful, violent and other illegitimate content;
  - Any other functionalities or services not explicitly made part of the target of evaluation in this ToE description;
- 3rd party single sign-on (e.g., Google, Facebook, Twitter);
- Customer support services provided by Aspiegel SE or any of their affiliates or 3rd parties;
- Hardware and software used by consumers who access the HUAWEI ID service;
- HUAWEI ID as it is provided to users outside the EU/EEA.

Meaningful Graphical Illustration of the data flow

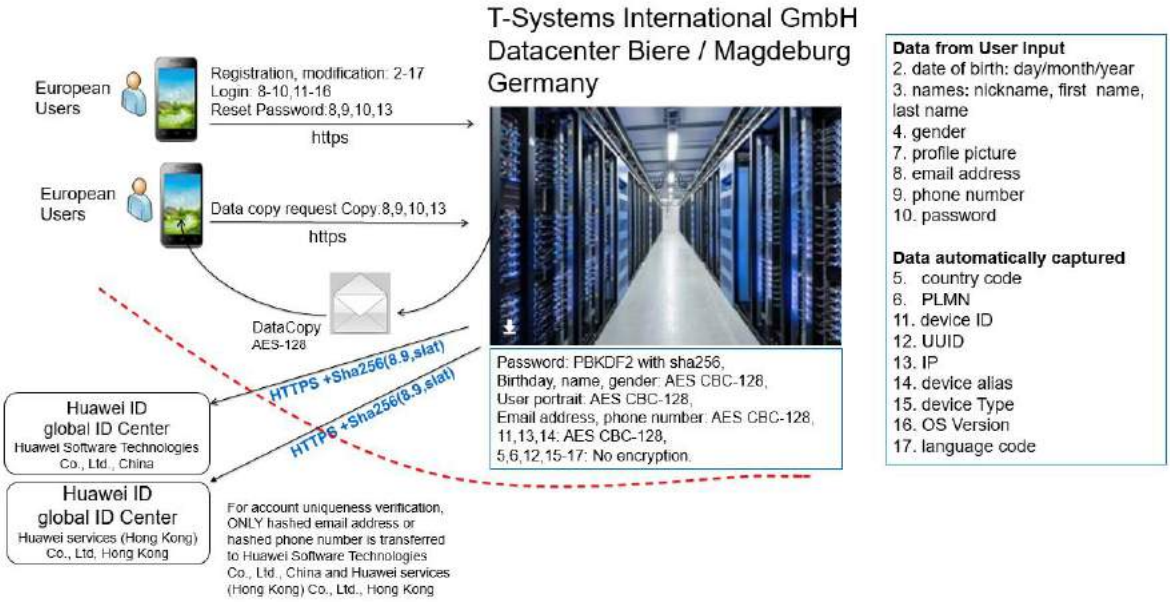

Fig 6: Data Flow Diagram

PLMN:	Public Land Mobile Network
UUID:	Universally Unique Identifier
PBKDF:	Password Based Key Derivation Function
AES CBC:	Advanced Encryption Standard Cipher Block Chaining Mode
SHA:	Secure Hash Algorithm

4. Requirement Profile

1. Overview of Fundamental Issues	**Applicable or Not Applicable**
1.1.1 Processing Operations; Purpose(s)	Applicable
1.1.2 Processed Personal Data	Applicable
1.1.2.1 Personal Data	Applicable
1.1.2.2 Special Categories of Data	Not applicable
1.1.2.2 Personal Data Relating to Criminal Convictions and Offences	Not applicable
1.1.3 Controller	Applicable
1.1.4 Transnational Operations	Applicable
1.2.1 Data Protection by Design and by Default	Applicable
1.2.1.1 Data Protection by Design	Applicable
1.2.1.2 Data Protection by Default	Applicable
1.2.2 Transparency	Applicable
1.2.2.1 Transparency and Description of the Product or Service	Applicable
1.2.2.2 Special Case: Privacy Notice	Applicable
2. Legitimacy of Data Processing	**Applicable or Not Applicable**
2.1.1 Legal Basis for the Processing of Personal Data in General	Applicable
2.1.1.1 Processing on the Basis of Consent	Applicable
2.1.1.2 Processing on the Basis of a Contract	Applicable
2.1.1.3 Processing on the Basis of Legal Obligation	Not applicable
2.1.1.4 Processing on the Basis of Vital Interests	Not applicable
2.1.1.5 Processing on the Basis of a Public Task	Not applicable
2.1.1.6 Processing on the Basis of Balancing of Interests	Applicable
2.1.2 Legal Basis for the Processing of Sensitive Personal Data	Not applicable
2.1.2.1 Processing of Sensitive Data on the Basis of Explicit Consent	Not applicable
2.1.2.2 Processing of Sensitive Data in the Field of Employment, Social Security and Social Protection Law	Not applicable
2.1.2.3 Processing of Sensitive Data: Vital Interests	Not applicable
2.1.2.4 Processing of Sensitive Data for a Not-For-Profit Body	Not applicable
2.1.2.5 Processing of Published Sensitive Data	Not applicable
2.1.2.6 Processing of Sensitive Data for the Defence of Legal Claims	Not applicable
2.1.2.7 Processing of Sensitive Data for Reasons of Substantial Public Interest	Not applicable
2.1.2.8 Processing of Sensitive Data for Medical and Related Purposes	Not applicable
2.1.2.9 Processing of Sensitive Data for Public Health Reasons	Not applicable
2.1.2.10 Processing of Sensitive Data for Archiving, Research or Statistical Purposes	Not applicable
2.1.2.11 Processing of Genetic Data, Biometric Data or Data Concerning Health	Not applicable
2.1.3 Processing of Personal Data Relating to Criminal Convictions and Offences	Not applicable
2.1.4 Provisions Relating to Specific Processing Situations	Not applicable
2.1.4.1 Processing of Data for the Sole Purposes of Journalism or Artistic or Literary Expression	Not applicable
2.1.4.2 Processing and Public Access to Official Documents	Not applicable
2.1.4.3 Processing of National Identification Numbers and other General Identifiers	Not applicable
2.1.4.4 Processing in the Context of Employment	Not applicable
2.1.4.5 Processing for Archiving Purposes in the Public Interest, Scientific or Historical Research Purposes or Statistical Purposes	Not applicable
2.1.5 Special Restrictions on Certain Data Processing under the ePD (ePrivacy Directive)	Applicable
2.1.5.1 Special Restrictions on the Use of Cookies and other Information Stored in the Terminal Equipment of a Subscriber or User	Applicable
2.1.5.2 Special Restrictions on the Processing of Traffic Data	Not applicable
2.1.5.3 Special Restrictions on the Processing of Location Data	Not applicable
2.1.5.4 Special Restrictions on the Making of Unsolicited Direct Marketing Contacts with Subscribers	Applicable
2.2.1 Record of Processing Activities	Applicable

2.2.2 Designation of a Data Protection Officer	Applicable
2.2.3 Designation of a Representative in the EU	Not applicable
2.2.4 Data Protection Impact Assessment	Applicable
2.2.5 Prior Consultation	Not applicable
2.2.6 Notification of a Personal Data Breach	Applicable
2.2.7 Processing under the Authority of the Controller or Processor	Applicable
2.3.1 Data Collection (Information Duties)	Applicable
2.3.2 Internal Data Disclosure	Applicable
2.3.3 Disclosure of Data to Third Parties	Applicable
2.3.4 Erasure of Data after Cessation of the Requirement	Applicable
2.4.1 Processing of Data by Joint Controllers	Not applicable
2.4.2 Processing of Data by a Processor	Applicable
2.4.3 Transfer to Third Countries	Applicable
2.4.4 Automated Individual Decisions	Not applicable
2.4.5 Processing of Personal Data Relating to Children	Applicable
2.4.5.1 Conditions Applicable to Child's Consent in Relation to Information Society Services	Applicable
2.4.5.2 Consideration of the Need for Specific Protection of Children when Performing a Balancing of Interest Test	Applicable
2.4.5.3 Understandability of Information and Communication where Processing is Addressed to a Child	Applicable
2.4.5.4 Requirement that Automated Individual Decisions, including Profiling, Should not Concern a Child	Applicable
2.4.5.5 Consideration of the Need For Specific Protection of Children when Assessing the Risks of the Processing	Applicable
2.5.1 Lawfulness, Fairness and Transparency	Applicable
2.5.2 Purpose Limitation	Applicable
2.5.3 Data Minimization	Applicable
2.5.4 Accuracy	Applicable
2.5.5 Storage Limitation	Applicable
2.5.6 Integrity and Confidentiality	Applicable
2.5.7 Accountability	Applicable
3. Technical-Organisational Measures: Accompanying Measures for Protection of the Data Subject	**Applicable or Not Applicable**
2.1.1.1. Physical access control	Applicable
2.1.1.2. Access to media and mobile devices	Not applicable
2.1.1.3. Access to data, programmes and devices	Applicable
2.1.1.4. Identification and authentication	Applicable
2.1.1.5. Use of passwords	Applicable
2.1.1.6. Organisation and documentation of access controls	Applicable
2.1.2.1. Logging mechanisms	Applicable
2.1.2.2. Operation of the logging mechanisms	Applicable
2.1.3. Network and transport security	Applicable
2.1.4.1. General Measures	Applicable
2.1.4.2. Back-up mechanisms	Applicable
2.1.4.3. Backup storage	Applicable
2.1.4.4. Recovery mechanisms	Applicable
3.1.5.1 Security Policy	Applicable
3.1.5.2 Risk Analysis	Applicable
3.1.5.3 Documentation of Technical and Organisational Data Protection Measures	Applicable
3.1.5.4 Documentation of Individual Obligations	Applicable
3.1.5.5 Inventory of Hardware, Software, Data and Media	Applicable
3.1.5.6 Media Management	Applicable
3.1.5.7 Appointment and Duties of Data Protection or Security Officers	Applicable
3.1.5.8 Instruction and Confidentiality of Personnel	Applicable
3.1.5.9 Data Protection and Security Audit	Applicable
3.1.5.10 Incident Management by Manufacturers and Operators	Applicable
3.1.5.11 Test and Release	Applicable
3.1.6 Disposal and Erasure of Data	Applicable
3.1.7 Temporary Files	Applicable

3.1.8 Documentation of Products and Services from a Customer's Perspective	Applicable
3.2.1 Encryption	Applicable
3.2.2 Pseudonymization and Anonymization	Applicable
3.2.3 Technical Data Protection Functionalities Required by the ePrivacy Directive (ePD)	Not applicable
3.2.4 Ensuring Transparency of Automated Individual Decisions	Not applicable
3. Data Subjects' Rights	**Applicable or Not Applicable**
4.1.1.1 Information Provided to Data Subjects when Data are Collected from Them Directly	Applicable
4.1.1.2 Information Provided to Data Subjects when Data are Collected from Other Sources	Not applicable
4.1.2 Right of Access	Applicable
4.1.3 Right of Correction	Applicable
4.1.4 Right of Erasure	Applicable
4.1.5 Right to Restriction of Processing	Applicable
4.1.6 Right to Data Portability	Applicable
4.1.7 Right to Object	Applicable
4.1.8 Right not to be Subject to Automated Individual Decision- Making	Not applicable
4.1.9 Right to be Informed of Personal Data Breaches	Applicable
4.1.10 Processing Which Does Not Require Identification	Not applicable
4.2.1 The Right to be Informed of Personal Data Breaches	Not applicable
4.2.2 The Right to be Informed of Security Risks	Not applicable
4.2.3 The Right to Confidentiality of Communications	Not applicable
4.2.4 The Right to Receive Non-itemized Bills	Not applicable
4.2.5 The Right to Prevent Calling-line and/or Connected Line Identification and Call Forwarding	Not applicable
4.2.6 Special Rights Regarding Directories of Subscribers to Electronic Communications Services	Not applicable

5. Overview of Evaluation Methods

5.1. Document Review

Legal Documents related to the ToE	
Document Type	**Remark**
Record of Processing Activities	OK
Designation Certificate of the Data Protection Officer (DPO)	OK
Further DPO Related Documentation	Not applicable
Proof of Designation of a Representative in the EU	Not applicable
Retention Policy	OK
Data Breach Notification Concept	OK
Results of the Data Protection Impact Assessments (DPIA)	Barely passing
Privacy Notice	OK
Cookie Notice	OK
Terms of Service (ToS)	OK
List of (Sub) processors with ToE Relevance and Their Location	OK
Documents re the Selection of Processors in General	OK
Document/s Demonstrating Careful Selection of Each Processor	OK
Signed Data Protection Agreement/s (DPA)	OK
Signed Joint Controller Agreement/s (JCA)	Not applicable
Consent Form	OK

Results of Balancing Tests	OK
Results of Transfer Impact Assessments (TIA)	OK
Other Documents Related to Transfer to a Third Country	OK
Work Instruction re Data Subject Requests	OK
Work Instruction re Cooperation with Supervisory Authority	OK

Technical Documents related to the ToE	
Document Type	**Remark**
Data Flow Diagram	OK
Documentation regarding Technical and Organisational Measures (TOMs)	OK
Log Data	OK
Evidences of Relevant Certifications	OK
Evidence of Relevant Audits/Inspection	OK

Other Documents related to ToE	
Document Type	**Remark**
Information Sheets, User's Manual or Similar	OK

EuroPriSe specific Documents	
Document Type	**Remark**
Application for Certification	OK
ToE Description	OK
Results of Risk Analysis	OK
Results of Maturity Assessment	OK
Affirmation Declaration	OK

5.2. Interviews

Legal Interviews were conducted with John Suffolk (Data Protection Officer) and Jingjing Wang (Product Development Manager) regarding the following topics:

- Potential issues in HUAWEI ID creation from data protection perspective
- Data transfer to 3rd Country

Technical interviews were conducted with Jian Wu (Principle Privacy Engineer) and Xiong Qinhui (System Engineer) regarding the following topics:

- Encryption
- Server hardening
- Backup and recovery mechanism
- Log handling

5.3. Test Accounts

Multiple test accounts have been created on the HUAWEI ID portal (both from web and mobile device) for the purpose of legal and technical evaluation. During the process of creating and using the test accounts, necessary checks have been performed to ensure that adequate measures are in place.

5.4. Use of Tools

SSLLabs has been used to test the following topics

- Encryption
- Digital certificates

6. Results

6.1 Result of Legal and Technical Evaluation

The main results of the legal and technical evaluation can be summarised as follows:

Legal Evaluation

Legal Basis

With regard to the mandatory data, the service provider can refer to the legal basis of Art. 6(1)(1)(b) GDPR. All data specified as mandatory are necessary in order to create and use a HUAWEI ID account and to guarantee the integrity and confidentiality of this account. In respect of the latter purpose (guarantee integrity and confidentiality), it could be argued that not Art. 6(1)(1)(b) GDPR, but Art. 6(1)(1)(f) GDPR is the appropriate legal basis. Even then, the data processing would be permissible, since the service provider has a legitimate interest in the secure processing of the personal data, the processing is necessary for this purpose and the interests of the data subjects against this data processing do not override the interests of the service provider (rather, secure processing is in the interest of the data subjects, too). This legal assessment is in line with the "Guidelines 2/2019 on the processing of personal data under Article 6(1)(1)(b) GDPR in the context of the provision of online services to data subjects" (Version 2.0) published in 2019 by the European Data Protection Board (EDPB).

For the fields marked as optional, the service provider can rightly refer to the legal basis of Art. 6(1)(1)(f) GDPR. The service provider has an interest in making the use of HUAWEI ID as convenient and user-friendly as possible for the user. No conflicting predominant interests of the users are apparent. Rather, users are free to decide whether to provide the optional details. If a user has provided information on an optional data field, it can be assumed that there is no conflicting interest on the part of the data subject, especially as the user can delete the information at any time.

With regard to the permission for minors to create an account without the respective legal guardian, the service provider adheres to the age limits for the validity of the consent of minors that have been stipulated by the EU member states based on Art. 8(1)(2) GDPR. Even if the processing of personal data with regard to HUAWEI ID is not based on consent, it may legitimately be based on the relevant age regulations in the EU member states and is applied as a "best practice" standard in the field of online services.

The service provider also uses the personal data of adult users for marketing purposes. This is done in a GDPR compliant manner. The legal basis in this respect is also Art. 6 (1)(1)(f) GDPR. However, this is for internal use only, for example to compare the development of user numbers in European countries in the area of business development.

It should also be noted that direct marketing, such as contacting a user directly for advertising purposes, only takes place with the consent of the data subject. Direct marketing is only addressed to adults, but not to minors. Since it is always based on the informed consent of the data subject, data processing related to direct marketing activities takes place on a valid legal basis.

Secondary data such as logging data is processed in a legally permissible manner as well. The purpose of this processing / storage is to guarantee the integrity and confidentiality of the service. The legal basis for this is Art. 6(1)(1)(b) GDPR / Art. 6(1)(1)(f) GDPR (cf. already above). With regard to retention obligations, the legal basis is Art. 6(1)(1)(c) GDPR.

Cookies

A part of the ToE (the web portal) is provided via the internet. In this context, Aspiegel SE makes use of cookies. All cookies used are strictly necessary to provide the respective services. No tracking cookies are used. According to the requirements of Art. 5(3) of the ePrivacy Directive in the current version (as amended by Directive 2009/136/EC), consent is not required in this respect.

Use of Processors

Data processing agreements (DPAs) have been concluded with all service providers who process personal data as processors on behalf of Aspiegel SE. These agreements comply with the requirements of Art. 28 GDPR.

Transfer to 3rd Countries

As already outlined above, in order to ensure global uniqueness of HUAWEI account, very limited information is synchronised across different sites providing HUAWEI ID accounts. It is worth noting that only pseudonymised data (in concrete: a unique HUAWEI ID number as well as the hashed phone number and email address of the user) is used for this purpose. This pseudonymous information is transferred to China as well as Hong Kong, Malaysia, Russia, and Singapore. The respective transfers are legitimised by standard contractual clauses (SCC) signed with the respective service providers as well as the supplementary measure of pseudonymisation / hashing.

Aspiegel SE submitted a transfer impact assessment (TIA) addressing the 3rd country transfers for the purpose of uniqueness verification, which meets the respective requirements of the applicable criteria catalogue.

Transparency

The privacy notice as well as the cookie notice are in line with the legal requirements.

Technical Evaluation

Physical access control

Aspiegel SE has the responsibility for the physical security of T-Systems (data centre), where appropriate technical and organisational measures have been implemented according to ISO27001 (valid certification with a renewal contract).

Authentication and Authorization

To prevent unauthorized access to any data, Aspiegel SE has implemented adequate security measures (2-factor authentication, use of captcha, state-of-the-art password management) for the use of HUAWEI ID.

Documentation of Access Controls

Access rights are properly organized and well documented under the control of the ISO27001 process of HUAWEI. All rules and regulations for access administration are explained within the policy/regulation documentation.

Logging

There are multiple types of logs (server systems, operation, database, access administration, activity, application) generated in several places, that contain personal data. For each type of logs, all the procedures (creation, storage, retention, deletion, recovery, management) are well documented in the policies.

Network and Transport Layer Security

Aspiegel SE has defined all the infrastructural and security details regarding network communication (Virtual Private Network, Firewalls, Intrusion Detection/Prevention Systems) along with the transport layer security.

Backup and Recovery

There is no such backup mechanism implemented within the smartphone. All data are stored at the data centre of T-Systems. They have implemented adequate measures (business continuity management, backup concept, backup type, and medium, frequency, and disaster recovery) to manage backup and recovery mechanisms according to the state-of-the-art standards.

Handling of Temporary Files

There is a separate functionality on the HUAWEI portal to create and manage the temporary files, which stores the copy of user’s personal data for a specific period and gets removed automatically afterwards.

Pseudonymization and Anonymization

For uniqueness verification, hashed phone number and email address of the users are transferred to China as well as Hong Kong, Malaysia, Russia, and Singapore. For this purpose, (Secure Hash Algorithm) SHA-256 is used which is state-of-the-art technique.

OVERALL RESULT:

The overall result of the evaluation is “passed” (i.e. that the target of evaluation meets all applicable requirements from the EuroPriSe Criteria Catalogue for the certification of IT products and IT-based services (v201701)).

On behalf of the evaluation team:

Place, Date	Name of the Lead Evaluator	Signature

6.2 Result of Legal and Technical Review of Evaluation Results

The review team has reviewed all information and results related to the evaluation. The overall result of the review is “passed” (i.e. that the target of evaluation meets all applicable requirements from the EuroPriSe Criteria Catalogue for the certification of IT products and IT-based services (v201701)).

Place, Date	Name of the Lead Reviewer	Signature