Short Public Report

1. Name and version of the IT-based service:

    HUAWEI ID as provided to users in the EU/EEA by Aspiegel Limited in 01/2020

    (classification: controller service)

2. Provider of the IT-based service:

    Company Name:

    Aspiegel Limited

    (a wholly owned subsidiary of Huawei Technologies Cooperatief U.A (Netherlands))

    Address:

    Simmonscourt House

    Ballsbridge

    Dublin

    D04 W9H6

    IRELAND

    Contact Person:

    Jie Su and Jian Wu

3. Time frame of evaluation:

    September 15th, 2016 to January 27th, 2020

4.   EuroPriSe Experts who evaluated the IT-based service:

Name of the Legal Expert:

Stephan Hansen-Oest

Address of the Legal Expert:

Rechtsanwalt Stephan Hansen-Oest

Im Tal 10a

24939 Flensburg

Germany

sh@hansen-oest.com

Name of the Technical Expert:

Andreas Bethke

Address of the Technical Expert:

Andreas Bethke

B³ | Informationstechnologie

Papenbergallee 34

25548 Kellinghusen

Germany

bethke@europrise-expert.com

5.   Certification Body:

Name: EuroPriSe Certification Authority

Address: Joseph-Schumpeter-Allee 25

53227 Bonn

Germany

eMail: contact@european-privacy-seal.eu

6.   Specification of the Target of Evaluation (ToE):

Aspiegel Limited 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, Honor store, etc. as well as to (3rd party) apps.

The ToE of this certification is HUAWEI ID as it is provided by Aspiegel to users in the European Union (EU)/European Economic Area (EEA).

Other mobile services or apps provided by Aspiegel or any of their affiliates do not form part of this target of evaluation. The same holds true for (3rd party) apps that may interact with HUAWEI ID. More precisely: The ToE covers only the registration, storage and administration of the HUAWEI ID by using a mobile device (smart phone client) or a web browser (web portal), but not a possible disclosure of data from the HUAWEI ID service to other services / (3rd party) service providers. In other words: The 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.

The ToE includes:

- HUAWEI ID Client as an integrated service app in Huawei Android devices;

- HUAWEI Mobile Services APK to the extent it is required for the use of HUAWEI ID (but not for any other mobile services);

- The HUAWEI ID web portal: https://id7.cloud.huawei.com/CAS/portal/login.html;

- Backend server;

- Captcha server;

- The single sign-on service (SSO) as it is provided by Aspiegel (as such – cf. above);

- All processes and interfaces concerning the registration, storage and administration of the HUAWEI ID by using a mobile device (smart phone client) or a web browser (web portal);

- All processes and interfaces related to the processing of personal data for (direct) marketing and business development purposes to the extent it is directly related to the ToE as such.

Exclusions and restrictions regarding the ToE:

- Other mobile services provided by Aspiegel or any of their affiliates or any 3rd parties are out of scope of this certification (cf. already above).

- The function "find my phone" is not part of the ToE.

- The function "my address" may be implemented in the future, but is not part of the ToE right now.

- HUAWEI ID as it is provided to users outside the EU/EEA is not covered by this certification.

- It is possible to store credit card data in the HUAWEI ID account. However, this is not mandatory. The storage of credit card data is not part of the ToE.

- It is possible to make use of single sign-on (SSO) options provided by 3rd parties (Google, Twitter, WeChat and Facebook). These third party SSO options are excluded from the ToE.

- Customer support services provided by Aspiegel or any of their affiliates or 3rd parties are out of scope of this certification.

- This certification does not cover the hardware and software used by the users of the HUAWEI ID service (with the exception of the ToE itself of course).

7. General description of the IT-based service:

HUAWEI ID is a service of the service provider Aspiegel Limited, a wholly owned subsidiary of Huawei Technologies Cooperatief U.A (Netherlands). The service provider offers HUAWEI ID in order to enable users of mobile devices with an Android operating system to register and / or log in with other services using a "HUAWEI ID". In this respect, the ToE may be considered a "single sign-on" (SSO) solution. The services that can be used with a HUAWEI ID include services such as the AppGallery, Mobile Cloud, Developer Alliance, Video, Browser, Assistant, Music, Themes, Honor store, etc. as well as (3rd party) apps.

However, the HUAWEI ID is not only used to access services. It also serves the purpose to protect the users of HUAWEI ID. For example, if a user logs in to a certain service with the HUAWEI ID and tries to log in from a different device than before, the user may be informed of this for security reasons, e.g. via an SMS containing a verification code, and will then be in the position to allow or deny access accordingly (2 factor authentication).

The HUAWEI ID is offered globally in different variations. The certification refers only to the version that is provided to users in the EU/EEA.

I. **Creation of a HUAWEI ID Account:**

To create a Huawei ID, the user must register. The user can choose between registering with a phone number or with an email address (for details see below). Accordingly, the confirmation of the registration will be sent either by email or by phone.

A SIM card is not mandatory to use the service. If a SIM card is used, the service provider uses the first three digits of the IMSI (international mobile subscriber identity) stored on the SIM card to identify the language and country of the user and to offer the services in the appropriate language and configuration. In addition, the phone number (specified during registration or later in the profile) is only used to send/receive SMS codes that are necessary for, e.g., login or registration.

Figure 1- Registration with phone number

Figure 2- Registration with email address

Registration for a HUAWEI ID is also possible via 3rd party service providers such as Twitter, Google, WeChat and Facebook. However, these possibilities are not part of the target of evaluation (cf. the ToE section above).

The date of birth is required, since minors up to a certain age, which may vary from country to country, are excluded from registering a HUAWEI ID by themselves (cf. below at no. 12 evaluation results). There is no further mechanism for age verification in place.

Each time a new account is registered, confirmation from the account holder is required via smartphone or email.

Before completing the registration, the links to the data protection statement and the cookie notice for the ToE are displayed and the user must accept the terms of service for HUAWEI ID.

The service provider uses "captcha software", which serves the purpose to ensure that the account registration or login is carried out by a human and not by a machine (e.g. a "bot").

The tool "GeeTest" is used for this purpose. It is operated on the service provider's own servers (i.e. no 3rd party is involved here). GeeTest is used to determine mouse movements and typing speeds when solving the particular captcha challenge. The respective data is deleted immediately after the completion of the challenge. To ensure transparency vis-à-vis the user, s/he can access information on GeeTest directly in the captcha box. This information is provided on mouse-over action in relation to a dedicated icon (cf. figure 3 and 4 below). Additional information is presented within the privacy statement (website) for the ToE.

The relevant extract from the data privacy statement reads as follows:

If you visit the HUAWEI ID web portal, the following data shall be collected:

•Browser network and usage information: such as data stored by cookies (such as your session ID, login status, HUAWEI ID account region, login QR code, page style settings, CAPTCHA code and status, random identifier of your browser, encrypted account user name), IP address, mouse and keyboard activities on the page, browser type, time zone, language and font. The processing of your mouse and keyboard inputs is done for the purposes of account security and CAPTCHA to test whether a robot or a human operates the browser.

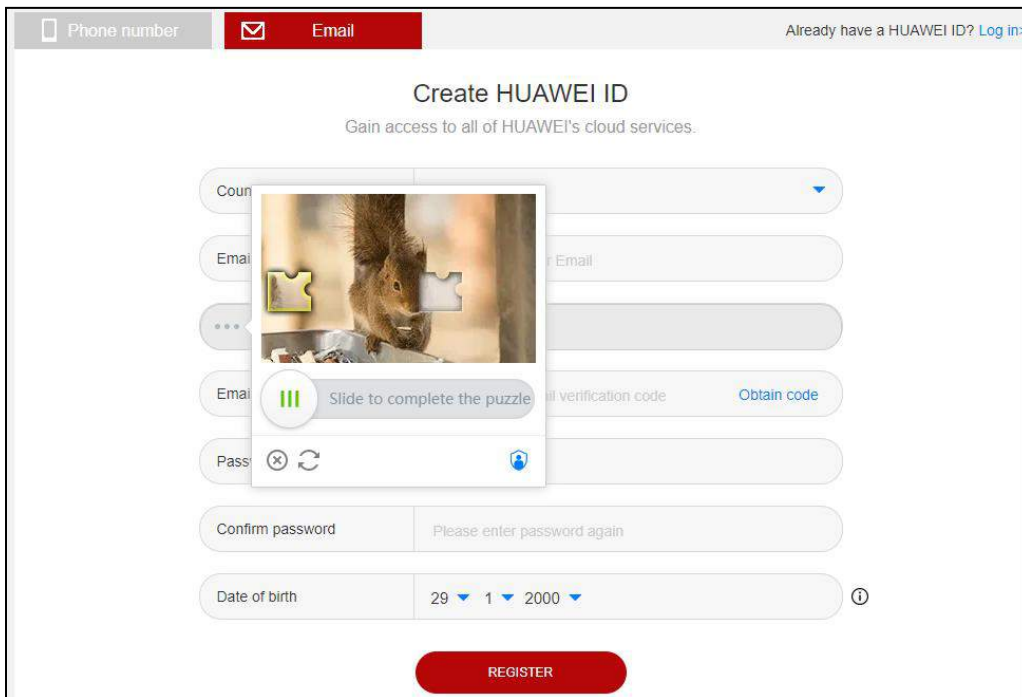Within the captcha functionality itself, information is provided to the users as shown below:

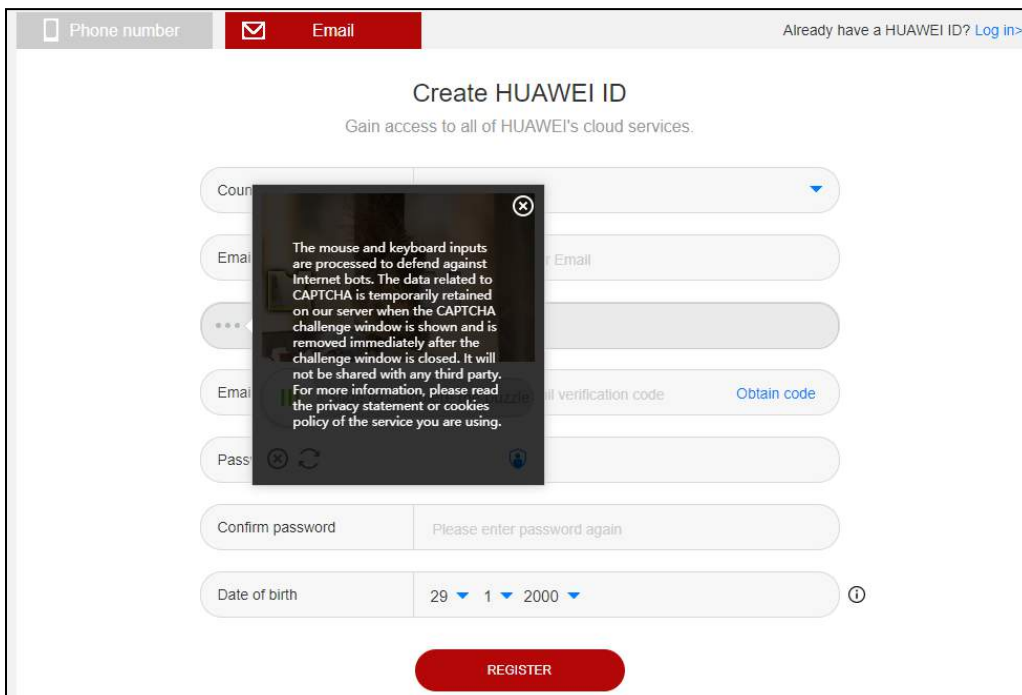*Figure 3 - Information about GeeTest captcha (I)*

Figure 4- Information about GeeTest captcha (II)

II.   Use of a HUAWEI ID Account

Login to the service (via App or Website)

The user can login to the service on a HUAWEI smartphone or via web portal. In both cases, users can authenticate themselves by means of phone number / email address / login ID and a password.
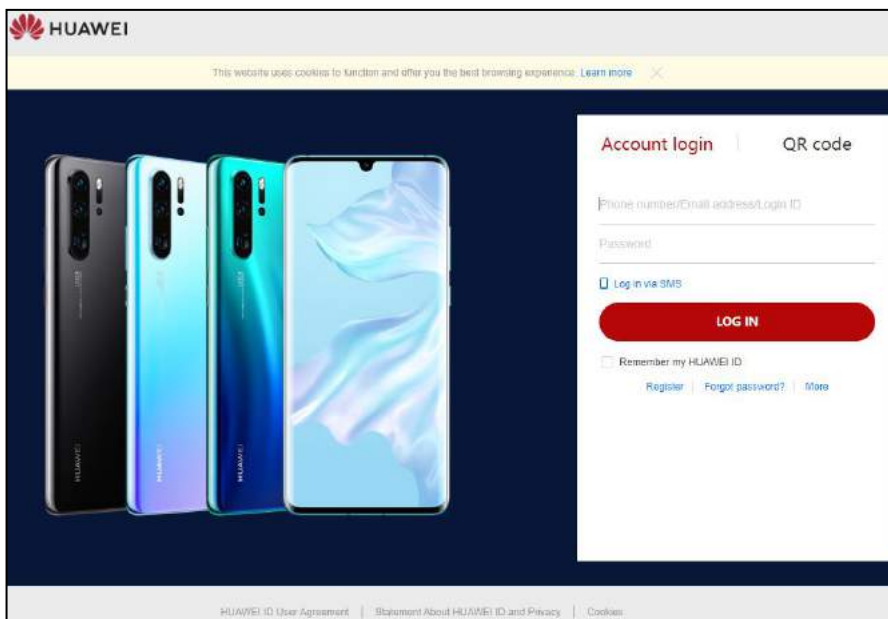
Figure 5 – Login with phone number / email address / login ID and password

As an alternative, the user may login with the aid of a QR-Code. This enables users to login via another Huawei device that is not (yet) registered. This QR code based login is also available for logins via the HUAWEI ID web portal (https://id7.cloud.huawei.com/CAS/portal/login.html).

When using the QR code, this code is displayed on the not (yet) registered device or the HUAWEI ID login website. It must be scanned with the already registered mobile device in order to log in as an authorised user.

Figure 6 - Login with a QR code

Available functionalities

After an account for the HUAWEI ID has been created successfully, the following main functions are available to the user:

- Login;

- Logout;

- Password management;

- Profile photo / nick name;

- Request your data;

- Delete account;

- Create child account;

- Secure identification.

Note: Secure identification via a security phone number or a security email address may be relevant if a device has been lost and, e.g., a phone number is bound to the lost device for getting SMS codes. In this case, another phone number (the security phone number) could be entered to reset the account.

Screenshots relating to the respective functionalities of the ToE are presented below:
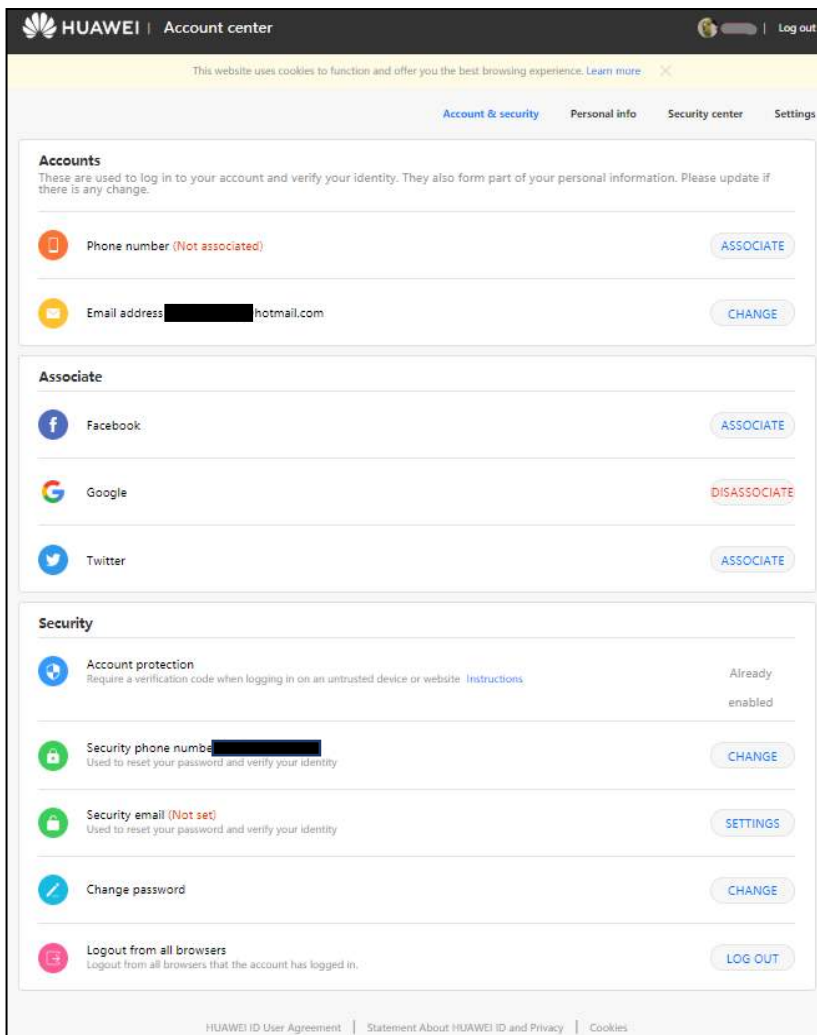

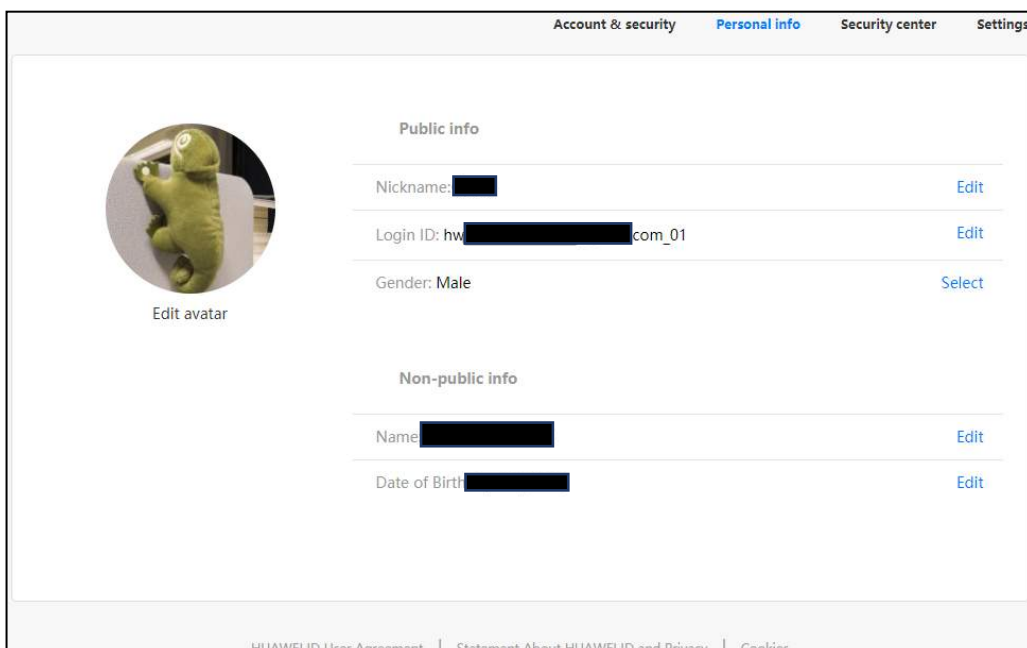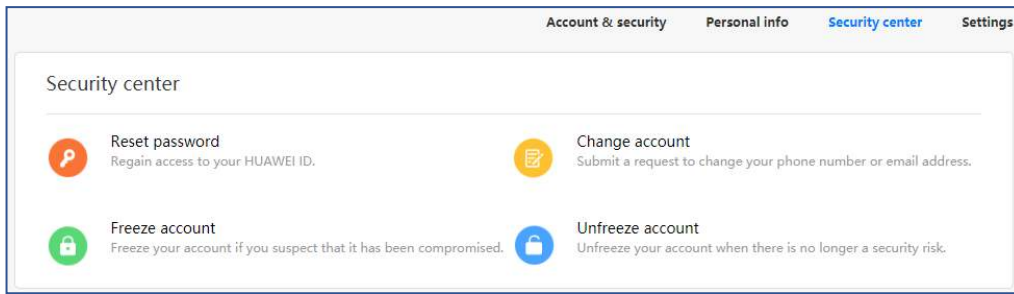*Figure 7 - Account & Security*

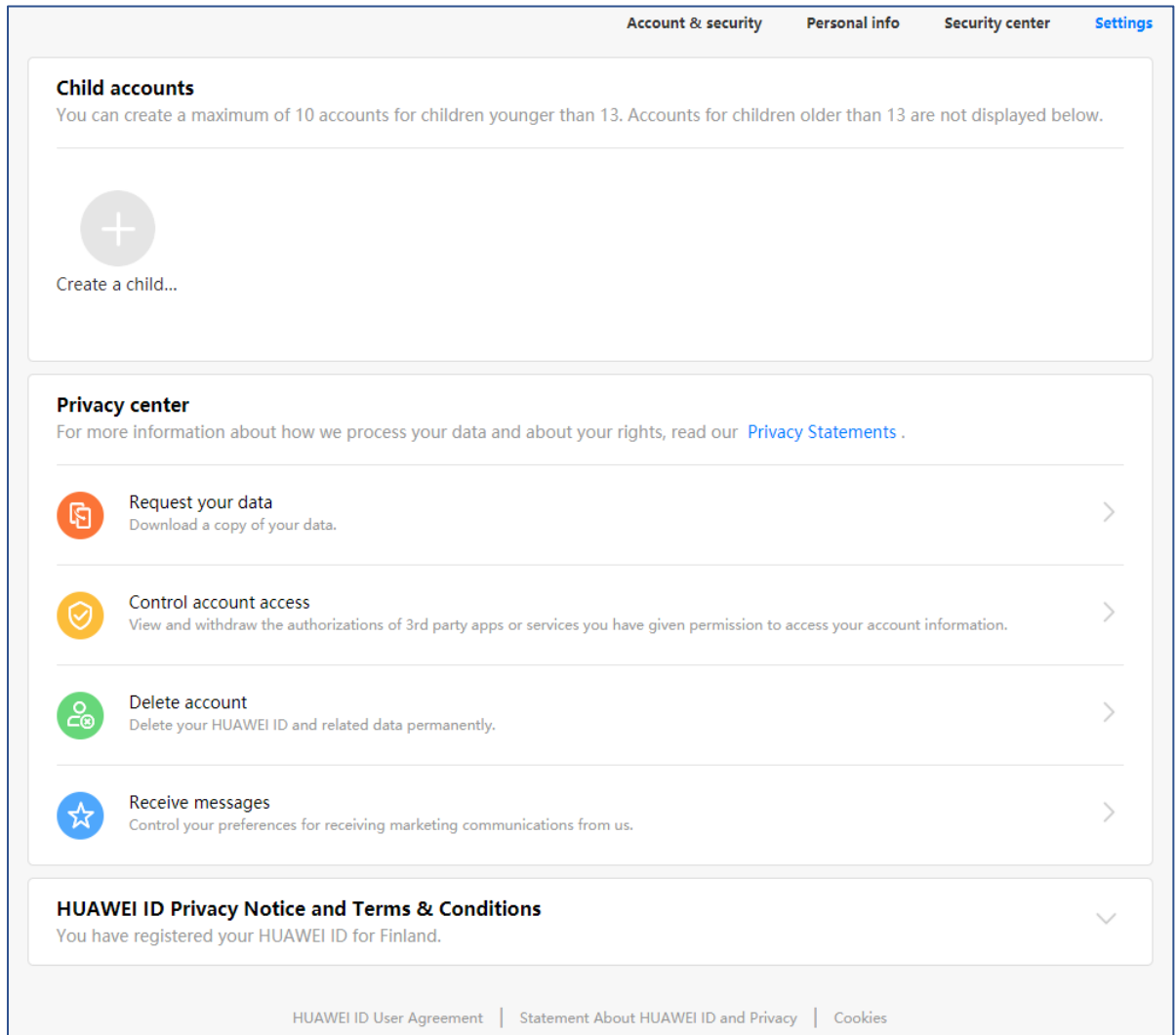*Figure 8 - Personal info*

Figure 9 - Security centre

Figure 10 - Settings

Overview on the SSO process for HUAWEI ID

When using the HUAWEI ID as an SSO solution to access other services, the process is as follows:

1. Encryption key will be exchanged between server and client by https before the real client-server data exchange happens.

2. User's account name and password is encrypted by the client using the previously exchanged key and the client sends a login request to the user profile (UP) server.

3. The user profile server decrypts the request and matches the account name and the hashed password with the values stored in the database. If this verification is successful, it passes the request to the account server (AS). The AS calls SSO to allocate the service token for this user.

4. The server replies the token to the client and the HUAWEI ID client keeps the service token.

5. HUAWEI ID allocates the service token to business services, such as AppGallery, Mobile Cloud, Developer Alliance, Video, Browser, Assistant, Music, Themes, Honor store etc.

6. When the business service uses HUAWEI ID login, the HUAWEI ID service will send the HUAWEI ID service token to the server of the business service.

7. The server of the business service submits the service token to the SSO server. After the SSO has verified the service token, it returns the userID (the unique number of the user's HUAWEI ID).

8. The server of the respective service has authenticated this user and the user is able to use the service.

Login to other services by means of HUAWEI ID

Once a user has successfully created a HUAWEI ID account, s/he can use it to log in to other Huawei services or to services of other providers if they support registration by HUAWEI ID.

If the HUAWEI ID is used to register for another service, data from the HUAWEI ID profile may be disclosed to the service provider after successful verification. The

disclosure of any data to another service and the processing of this data by the (3rd party) service provider is not subject of the ToE.

Technical Service Processes

In addition to the SSO functionality, the following service processes for the HUAWEI ID are implemented for use in the EU/EEA territory:

- Main service processes;

- Register a Huawei account from the HUAWEI ID client to the user profile server (UP server) using an email address;

- Register a Huawei account from the HUAWEI ID client to the UP server using a mobile phone number;

- Log in from the HUAWEI ID client to the UP server;

- Retrieve a password from the HUAWEI ID client to the UP server through a mobile phone number;

- Retrieve a password from the HUAWEI ID client to the UP server through an email address;

- Query and modify the user information from the HUAWEI ID client to the UP server;

- Query and modify a user profile picture and alias name (nickname) from the HUAWEI ID client to the UP server;

- Set a secure mobile phone number from the HUAWEI ID client to the UP server;

- Set a secure mailbox from the HUAWEI ID client to the UP server;

- Request account cancellation from the HUAWEI ID client to the UP server;

- Authenticate service token (ST) from the theme server to the UP server after the theme server obtains the service token;

- Query user information from the theme server to the UP server (depending on the actual service);

- Request personal data (including the activity log) from the UP server.

III. Processing by a processor

Aspiegel uses several service providers to process personal data as processors on its behalf. These are data centres, IT service providers and support service providers, namely

- T-Systems for data centre operations and IT service (system, server and application maintenance and operation, technical support);

- Huawei Technologies OY (Finland) for IT service (system, server and application maintenance and operation, technical support);

- Huawei Technology Software Co. Ltd. (China) for HUAWEI ID uniqueness validation;

- Huawei Technologies Dusseldorf GmbH for support services in EU, the sub-processor is Sykes Global Services Ltd.;

- Huawei Technologies Espana SL (Spain) for support services in Spain, the sub-processor is Teleperformance ESPANA S.A.U;

- Transcosmos Information Systems Ltd. (Warsaw) for support services in Poland.

The data centres used and the IT service providers are located in the European Union. This is different for Huawei Technology Software Co. Ltd., which is located in China. This processor has the sole task of validating the (worldwide) uniqueness of a HUAWEI ID (cf. below at no. 8 transational issues).

8. Transnational issues:

The certified service is offered in the EU/EEA only. Aspiegel uses the Chinese Huawei Technologies Co., Ltd as a processor. The processor has the sole task to validate the (worldwide) uniqueness of a HUAWEI ID. The processing is limited to the following data types: HUAWEI IDs, hashed email addresses and/or phone numbers of HUAWEI ID users. These data types are transferred to the processor to ensure that each email address and/or phone number is only registered once worldwide.

Aspiegel has concluded the EU Standard Contractual Clauses ("processors") with Huawei Technologies Co., Ltd. They form part of the Data Processing Agreement between Aspiegel Limited and Huawei Technologies Co., Ltd. The Appendixes 1 and 2 of the SCC have been filled with sufficient information regarding the processing operations etc. (Appendix 1) and relevant technical and organisational security measures implemented by Huawei Technologies Co., Ltd (Appendix 2).

9. Tools used by the provider of the IT-based service:

Please cf. annex 1 at the end of this document.

10. Edition of the EuroPriSe Criteria used for the evaluation:

EuroPriSe Criteria (IT products and IT-based services) – version January 2017

EuroPriSe Commentary – version May 2017

11. Evaluation methods:

The experts conducted the following evaluation methods:

The technical expert installed the HUAWEI ID on a Huawei Honor 8 smartphone (which was bought in a common way) and on a Nova 2 Plus smartphone (which was delivered by Aspiegel) and tested the features that form part of the ToE. Furthermore, he examined the data processing that takes place when the ToE is used (a) by means of the smartphone app and (b) by means of the web portal. This included an inspection of all

relevant log files. Moreover, the technical expert inspected a part of the source code from GeeTest CAPTCHA. Finally, he evaluated the technical and organisational measures implemented by Aspiegel and its processor T-Systems (data centre operations).

Aspiegel Ltd. provided comprehensive documentation regarding the service, the related processes and the implemented technical and organisational measures. The following documents formed part of the legal and technical evaluation:

- HUAWEI ID User Guide
- Aspiegel-Finland service agreement and Data Processing Agreement (DPA)
- Aspiegel-Huawei Technology Software Ltd Data Processing Agreement
- HUAWEI ID - deployment in CEE&Nordic and WEU
- Personal data collected by HUAWEI ID
- RFP-EuroPriSe (HUAWEI ID) V1.0-20160713
- DKBA 7552-2015.05 Security Standards for Key Management
- ISMS-2-01 Access Control Regulations 1
- ISMS-2-02 Business Continuity Management Regulations
- ISMS-2-06 Network Security Procedures
- ISMS-2-08 IT Operations Security Regulations
- ISMS-2-15 Security Management for Information Assets
- MBS_MIS_M006122 General Policy on Information Security V02.30
- MBS_MIS_MISE_M001031 Office Computers, Networks, Applications, Storage Media and Peripherals - Security Management
- MBS_MIS_MISE_R005540 Office Environment Security Management
- MBTIT_ITSM_SO_AM_R107832 Management Regulations Concerning System Account Password 4.0
- HUAWEI ID Server Key Management Design
- HUAWEI ID application Log
- CryptTool Installation Guide_V1.0
- 190205_Contract Mobile Service EU.doc
- 190205_Contract Mobile Service EU_Annex 1_Notes on commissioned processing of Personal Data.docx
- 190205_Contract Mobile Service EU_Annex 2_Benchmarking.docx
- 190205_Contract Mobile Service EU_Annex 3_1_SoC Technology.docx
- 190205_Contract Mobile Service EU_Annex 3_2_SoC Managed Service.docx
- 190205_Contract Mobile Service EU_Annex 3_3_SoC Privacy.docx
- 190205_Contract Mobile Service EU_Annex 4_1_Open Telekom Cloud Service Description.pdf
- 190205_Contract Mobile Service EU_Annex 4_2_1_Database Operations Check List.xlsx
- 190205_Contract Mobile Service EU_Annex 4_2_2_Database Operations_MySQL Standards.docx

- 190205_Contract Mobile Service EU_Annex 4_2_3_Database Operations_Cassandra Standards.docx
- 190205_Contract Mobile Service EU_Annex 4_2_Database Operations.docx
- 190205_Contract Mobile Service EU_Annex 4_3_Middleware Operations.docx
- 190205_Contract Mobile Service EU_Annex 4_4_Application Operation.docx
- 190205_Contract Mobile Service EU_Annex 4_5_Definition of service complexity.docx
- 190205_Contract Mobile Service EU_Annex 5_SLA Requirements.docx
- 190205_Contract Mobile Service EU_Annex 6_1_Pricing Requirements.docx
- 190205_Contract Mobile Service EU_Annex 6_2_Compensation and due date.docx
- Contract for IT Services regarding operation of EMUI EU_1000630457_signed
- Aspiegel ./. Huawei Technologies Dusseldorf GmbH Europe Data Processing Agreement (Sykes as subprocessor) – for customer support in most of European countries
- CSA STAR - certification paper (ISO 27001 - Certificate Huawei China)
- T-systems GDPR DPA_Aspiegel
- T-systems contact change request for Aspiegel – signed
- HwID assessment of requirement to carry out DPIA final
- HUAWEI ID User Agreement new - modified by Irish law firm MHC
- Records of Processing - HUAWEI ID
- Documents for the ISO 27001 Certification (Valid from 22.06.2016 until 21.01.2919 – last revision on 31.03.2018)
- 1st layer notice-HUAWEI ID EU site
- 2nd layer notice - HUAWEI ID Privacy Statement
- Contract for IT Services regarding operation of Mobile Service EU (Aspiegel ./. T-Systems)

12. Evaluation results:

When providing the HUAWEI ID service (EU/EEA only), Aspiegel Ltd. meets all applicable EuroPriSe requirements.

I. Processing of Personal Data

Processing operations and purposes

The following personal data are processed (mandatory data) / may be processed (optional data) when a user makes use of the ToE:

Mandatory data

- Registration country

=> This type of data is necessary for determining the contracting entity and the manner in which the service is provided to the user. If the user chooses a member state of the EU/EEA, the contracting entity is Aspiegel Limited and the services are provided to the user as outlined in this document. For users in non-EU member states, the contracting party and the actual design of the service may differ.

- Date of birth: day+month+year

=> In order to comply with the provisions for the protection of minors this piece of data can be considered as necessary.

- Email address or phone number

=> These are necessary account data. They are used for authentication and sending transactional messages, such as messages containing a verification code, confirming successful registration or information in the context of resetting a password, etc. The user can decide if s/he gives just an email address and/or a phone number. Users can modify these data at 'Personal info' in HUAWEI ID.

- Password

=> necessary account data for login authentication (only a hash value is stored in the database)

- Device Identifier

=> necessary identifier to identify an app on a device

Depending on the device and its emotion UI (EMUI) version, different identifiers will be processed:

UDID (unique device identifier) and SN (serial number) will be collected on new device models, such as P20, P30, MATE 30 or devices which have been upgraded to EMUI version 8.0 or higher;

A UDID is not available on some older device models, such as Huawei P8, Y3 or old devices with EMUI version under 8.0. In such a case, IMEI (international mobile equipment identity) and SN (serial number) will be collected;

Finally, MEID (mobile equipment identifier) or ESN (electronic serial number) will only be collected from very old legacy devices.

- Device alias name

=> necessary to identify a device

- Terminal type, OS version, language code

=> necessary to know a device's configuration to provide correct UI (user interface) to the user

- IP address

=> necessary for service & security audit and intrusion tracing.

Optional data

- Security email address or security phone number

=> Optional. If the user switches on account protection and specifies a security email address / phone number, this email address / phone number will be used for account security, such as recovering the account and receiving a verification code, if the user does not have access to the primary phone number and/or email address (anymore). Users are able to modify these data at 'Account and security' > 'Verification methods' in HUAWEI ID.

- Nickname

=> Optional account data to provide user services, if a user wants a nickname to be shown in other services, such as Themes, AppGallery, etc. The user can remove or modify the nickname at 'Personal info' in HUAWEI ID.

- User portrait

=> Optional account data to provide user services if a user wants a user portrait to be shown in other services, such as Themes, AppGallery, etc. The user can remove or modify the image in 'Edit profile picture'.

- Gender

=> Optional, if the user wants to input his/her gender in case the customer support contacts him/her.

- First name and last name

=> Optional, if the user wants to input his/her name in case the customer support contacts him/her. The user can remove or modify it at 'Personal info' in HUAWEI ID.

No special categories of personal data

Further types of personal data are not processed in the area of the ToE. In particular, the service provider does not intend to process any special categories of personal data within the meaning of Art. 9 GDPR.

Purposes

Aspiegel Limited processes the personal data mentioned above to provide the HUAWEI ID service as well as for IT security (e.g., prevention of unauthorised access by third parties) and (direct) marketing purposes (cf. below).

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.

Overall, it can be stated that the type, scope and duration of the data processing complies with the requirements of the GDPR.

Cookies

A part of the ToE (the web portal) is provided via internet pages. In this context, Aspiegel 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.

II.   Processing by a Processor

Data processing agreements have been concluded with all service providers who process personal data on behalf of Aspiegel Limited. These agreements comply with the requirements of Art. 28 GDPR. There are no legal objections against the use of these processors.

With regard to the processor in China (Huawei Technologies Co., Ltd), the service provider has ensured that appropriate guarantees for an adequate level of data protection are in place. Most importantly, the processor in China only receives the absolute minimum of data, which is required for the purpose of checking and guaranteeing the worldwide uniqueness of the HUAWEI ID account. Furthermore, Aspiegel Limited and Huawei Technologies Co., Ltd concluded the EU standard

contractual clauses, which form part of the Data Processing Agreement between those two parties.

III. Transparency

Aspiegel provides sufficient and comprehensible information about the purpose, manner and extent of its processing of personal data. It complies with the requirements for transparency of data processing and the information duties pursuant to Art. 12 ff. GDPR.

The information on the use of cookies meets the relevant legal requirement, too.

Users are adequately informed about the use of captcha technologies by means of an icon and further information provided on mouse over / when accessing the privacy statement for the ToE.

IV. Data Security

The service provider has implemented appropriate technical and organisational measures (TOM) as required by Art. 32 GDPR.

The hosting service provider used (T-Systems) and the data centres are certified according to ISO 27001, so that a basic level of security is ensured. Aspiegel itself also uses ISO 27001 standards, even though it is not (yet) certified. The company also orients itself to the technical and organisational measures specified by NIST.

Specifically with regard to the ToE, Aspiegel has implemented the following TOM, which meet the respective requirements according to EuroPriSe:

User accounts are always password protected. The passwords are always transmitted encrypted and (irreversibly) stored encrypted (as hash values).

Furthermore, some other data types are stored encrypted in the database as well. This includes:

- The email address and/or mobile phone number;

- The date of birth;
- The optional nickname and name;
- The optional profile picture;
- The optional gender;
- The device ID/IMEI and the device alias name;
- The IP address (of the device or computer used to access the service via app or browser).

Some other (non-personal / non-sensitive) data types are not stored encrypted, but in plain text. This includes:
- The Country Code;
- The PLNM (public land mobile network);
- The UUID (universally unique identifier);
- The terminal type;
- The language code;
- The OS (operating system) version.

For detailed information on this, see figure 10 below at no 13 data flow.

The device name (alias) multi-layer logging is also one of the technical measures implemented: On the one hand, logging is performed directly on the smartphone if a change is made to personal data. On the other hand, changes are also logged on the server side. Furthermore, there is an "activity log", which records when a user has reset the password, for example. The user can request this activity log either on the smartphone or on the website as part of the implementation of his or her rights as a data subject. Aspiegel makes the detailed log available to him/her within 7 days. Further logging generally takes place at the database level and at the operating system level, provided that administrative changes are made here. IP-adresses are obfuscated after 6 months in the activity log: the last octet (IP-V4) is deleted.

A data backup using an app on the smartphone itself is not planned, but all data is regularly backed up in the data centres using a comprehensive backup concept.

A risk analysis is part of the standard for the implementation of measures from ISO 27001. From this, the provider derives appropriate further measures, which are then regularly implemented and improved.

The service provider uses captcha technologies on its own servers to ensure that registration or login to HUAWEI ID is done by a human and not a machine. The scope of the processing is non-invasive. The use of this technology is required by Art. 32 GDPR to ensure the integrity and confidentiality of personal data. The associated data processing is permissible as a contractual accessory obligation according to Art. 6 (1)(1)(b) GDPR or pursuant to Art. 6(1)(1)(f) GDPR.

V.   Further requirements

The service provider maintains a record of processing activities pursuant to Art. 30(1) GDPR, which contains all legally required information regarding the ToE.

Aspiegel has appointed a data protection officer.

There is a defined process at the service provider for reporting any data protection incidents that may trigger reporting obligations under Art. 33 and 34 DSGVO.

In connection with the processing of personal data when using HUAWEI ID, Aspiegel informs the data subjects in a comprehensible and transparent manner.

Aspiegel stores personal data only for as long as it is necessary for the provision of its services and for the fulfilment of legal storage obligations in the respective EU member states. The service provider supports the protection of data subjects' rights by enabling the user to export personal data about him- or herself when using HUAWEI ID. The export is very detailed and extends to any other Huawei services that were used via HUAWEI ID (however, this is not part of the ToE for this certification).

As mentioned above, personal data is transmitted and stored in encrypted form. Furthermore, Aspiegel adheres to the principle of data avoidance and data economy, so that the provision of mandatory data is kept to a minimum and that the use of the service is possible without a SIM card and thus without providing a mobile phone number.
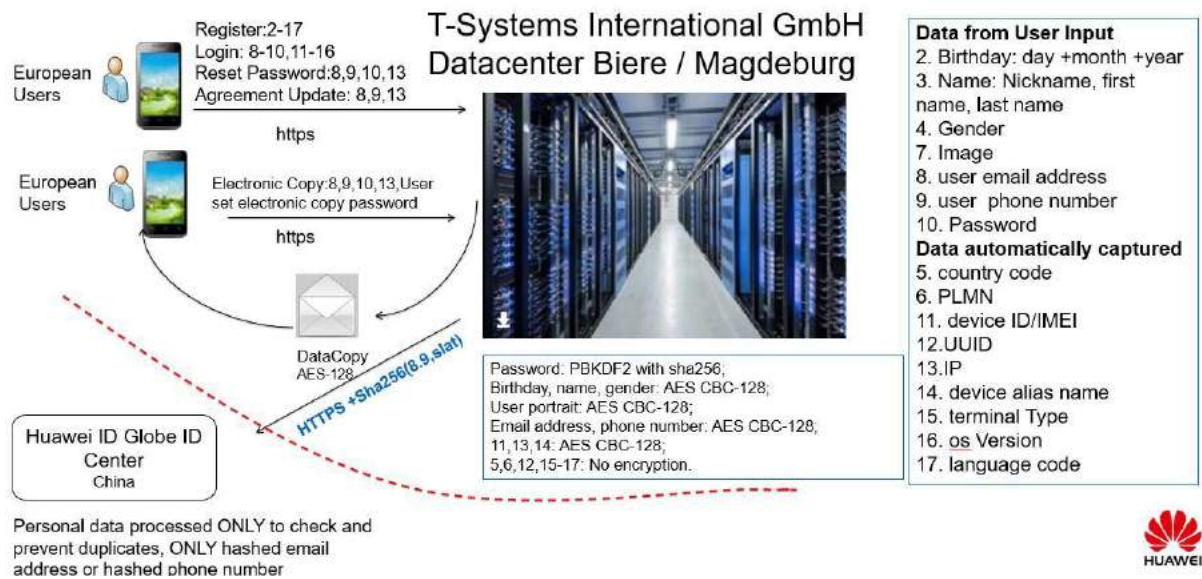
13. Data flow:

Figure 10 - Dataflow

14. Privacy-enhancing functionalities:

The service provider has made special efforts, particularly with regard to transparency, not only to meet the high requirements of the GDPR, but to partly exceed them. E.g., cf. the provision of information by means of a dedicated icon in the captcha context (cf. figures 3 and 4 above).

Another positive aspect is that the service provider has always aimed at processing less personal data than the usual industry standard.

15. Issues demanding special user attention:

None.

16. Compensation of weaknesses:

None.

17. Decision table on relevant requirements:

EuroPriSe Requirement	Decision	Remarks
Data Avoidance and Minimisation	*adequate*	Aspiegel strictly limits the processing of personal data that is mandatory for the HUAWEI ID service.
Transparency	*adequate*	The description and information on the service as such and on related data protection matters is understandable and comprehensive. It is available in several languages (depending on the user's country).
Technical-Organisational Measures	*adequate*	The manufacturer fulfils the legal requirements for technical and organisational measures for data security.
Data Subjects' Rights	*adequate*	Aspiegel complies with the legal requirements regarding data subjects' rights

_____

Experts' Statement

We affirm that the above-named IT product / IT-based service has been evaluated according to the EuroPriSe Criteria, Rules and Principles and that the findings as described above are the result of this evaluation.

Flensburg,

January 27th, 2020   Stephan Hansen-Oest

_____

Place, Date   Name of Legal Expert   Signature of Legal Expert

Kellinghusen,

January 27th, 2020   Andreas Bethke

_____

Place, Date   Name of Technical Expert   Signature of Technical Expert

Certification Result

The above-named IT product / IT-based service passed the EuroPriSe evaluation.

It is certified that the above-named IT product / IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection.

_____

Place, Date   Name of Certification Authority   Signature

ANNEX 1:

HUAWEI ID development software

- Eclipse 4.6.2 (and other compatible versions)
- Notepad++ 6.7.5 (and other compatible versions)
- Android Developer Studio version 3.2.x
- Approved java libraries that Huawei programmers can choose,

Memcached-Java-Client-3.0.2.jar
annotations-api.jar
ant-launcher.jar
ant.jar
apigw-client-sdk-2.0.0.200.jar
aspectjweaver.jar
async-http-client-1.9.15.jar
bcprov-jdk15on-159.jar
bcprov-jdk15on-160.jar
cassandra-driver-core-3.2.0-shaded.jar
cassandra-lucene-index-builder-3.0.14.0.jar
catalina-ant.jar
catalina-ha.jar
catalina-tribes.jar
catalina.jar
cloudsoa-lbs-sdk-1.0.2.300(SP1).jar
cloudsoa-mc-sdk-1.0.5.100.jar
cloudsoa-security-1.1.1.jar
com.huawei.dcs.basic-1.5.1.101.jar
com.huawei.dcs.commons-1.5.1.101.jar
com.huawei.dcs.dcsdk.core-1.5.1.101.jar
com.huawei.dcs.dcsdk.plugin.dmqsync-1.5.1.101.jar
com.huawei.dcs.dcsdk.support-1.5.1.101.jar
com.huawei.dcs.jetcd-1.5.0.101.jar
com.huawei.dcs.jetcd-1.5.1.101.jar
com.springsource.org.aopalliance-1.0.0.jar
commons-beanutils-1.9.3.jar
commons-cli-1.2.jar
commons-cli-1.3.1.jar
commons-codec-1.11.jar
commons-codec-1.9.jar
commons-collections-3.2.2.jar
commons-collections4-4.1.jar
commons-collections4-4.2.jar
commons-configuration-1.10.jar
commons-dbcp2-2.1.1.jar
commons-fileupload-1.3.3.jar
commons-io-2.5.jar
commons-io-2.6.jar
commons-lang-2.6.jar
commons-lang3-3.6.jar
commons-lang3-3.7.jar
commons-logging-1.2.jar
commons-net-3.6.jar

commons-pool-1.6.jar
commons-pool2-2.4.2.jar
commons-pool2-2.6.0.jar
core-3.3.3.jar
core-queue-client-1.9.31.jar
cryptutil-1.0.10.jar
cryptutil-1.2.0.jar
curator-client-4.0.0.jar
curator-framework-4.0.0.jar
curator-recipes-4.0.0.jar
datacopycenter-client-sdk-1.2.0.jar
devtestcov-ant-plugin-2.0.0-20170816.014447-2.jar
dmq-common-1.3.5.100.jar
dmq-mq-1.3.5.100.jar
dom4j-1.6.1.jar
druid-1.1.9.jar
dubbo-2.5.4-20150907.060938-1.jar
dubbo-2.6.0.jar
ecj-4.4.2.jar
el-api.jar
encryption-plugin2-1.0.6.jar
encryption-plugin2-1.0.7.jar
encryption-plugin2-NoSpring-1.0.7.jar
fastjson-1.2.40.jar
fluent-hc-4.5.5.jar
freemarker.jar
geoip-api-1.2.11.jar
guava-19.0.jar
hamcrest-core-1.3.jar
hprose-java-1.6.0.36.jar
httpclient-4.5.5.jar
httpclient-cache-4.5.5.jar
httpcore-4.4.9.jar
httpmime-4.5.5.jar
icu4j-59_1.jar
jackson-annotations-2.9.4.jar
jackson-core-2.9.4.jar
jackson-databind-2.9.4.jar
jasper-el.jar
javacc-5.0.jar
javassist-3.18.1-GA.jar
javassist-3.22.0-GA.jar
javax.mail-1.5.6.jar
jaxen-1.1.6.jar
jedis-2.9.0.jar
jetcd-2.2.8.jar
jmockit.jar
jopt-simple-3.2.jar
jsch-0.1.54.jar
jsp-api.jar
junit-4.12.jar
kafka-clients-0.10.1.1.jar
kafka-clients-0.8.2.1133101.jar
kafka_2.10-0.8.2.1132.jar

log4j-1.2-api-2.9.0.jar
log4j-1.2.17.jar
log4j-api-2.9.0.jar
log4j-core-2.9.0.jar
log4j-over-slf4j-1.7.25.jar
log4j-slf4j-impl-2.9.0.jar
log4j-web-2.9.0.jar
lz4-1.3.0.jar
metrics-core-2.2.0.jar
metrics-core-3.1.2.jar
mybatis-3.4.6.jar
mybatis-generator-core-1.3.6.jar
mybatis-spring-1.3.2.jar
mysql-connector-java-5.1.42.jar
netty-3.10.6.Final.jar
org.apache.servicemix.bundles.twitter4j-3.0.5_1.jar
poi-3.17.jar
rainbow-proxy-1.2.1.101.jar
scala-library-2.10.4.jar
sds-cassandra-auth-client-1.0.0.jar
sds-commons-2.0.1.101.jar
sds-lite-client-2.0.1.101.jar
service-adapter-sdk-1.3.28.jar
servlet-api.jar
slf4j-api-1.7.25.jar
slf4j-log4j12-1.7.25.jar
slf4j-nop-1.7.25.jar
slf4j-simple-1.7.25.jar
snappy-java-1.1.2.6.jar
spring-aop-4.3.18.RELEASE.jar
spring-beans-4.3.18.RELEASE.jar
spring-context-4.3.18.RELEASE.jar
spring-context-support-4.3.18.RELEASE.jar
spring-core-4.3.18.RELEASE.jar
spring-expression-4.3.18.RELEASE.jar
spring-jdbc-4.3.18.RELEASE.jar
spring-orm-4.3.18.RELEASE.jar
spring-test-3.2.13.RELEASE.jar
spring-test-4.3.5.RELEASE.jar
spring-tx-4.3.18.RELEASE.jar
spring-web-4.3.18.RELEASE.jar
spring-webmvc-4.3.18.RELEASE.jar
tomcat-api.jar
tomcat-coyote.jar
tomcat-dbcp.jar
tomcat-i18n-es.jar
tomcat-i18n-fr.jar
tomcat-i18n-ja.jar
tomcat-jdbc.jar
tomcat-util.jar
tomcat7-websocket.jar
uniaccount_batchimport.jar
upinterface.jar
userprofile_client.jar

userprofile_idmclient.jar
websocket-api.jar
xbean.jar
zip4j_1.3.1.jar
zkclient-0.3.jar
zookeeper-3.5.1-alpha.jar

Hardware

Aspiegel uses virtual machines that are hosted by T-systems. The following types of VM and disks that are used:

- VM Types: 4C8G , 8C18G and 16C128G
- Disk Types: High I/O (3 IOPS per GB/EVS disk) for disks and Ultra High I/O (50 IOPS per GB/EVS disk) for database

Operating system, middleware and database

- SUSE Linux Enterprise Server 11 Service Pack 3 - SuSE 11 sp 3
- MySQL version 5.6.24
- Java JRE version "1.8.0_74" and "1.7.0_91"
- Apache Tomcat Version 7.0.65
- NGINX nginx-1.10.1
- Openresty 1.3.1
- apache-cassandra-2.1.15
- redis-3.0.5