ePrivacyseal GmbH

Criteria Catalog

ePrivacyApp

(incl. requirements of EU-GDPR)

August 2016

The ePrivacyApp seal for data security and data protection from ePrivacyseal GmbH certifies for the respective applicant that its app is in line with the detailed criteria in the following criteria catalog based on the requirements of German and European data privacy law.

In particular, the observance of the following regulations is confirmed:

Part A

I. Formal requirements

The app is initially inspected as to whether the formal prerequisites of the proper reasoning and development of a contractual relationship for the installation on the terminal device of the user are fulfilled. Of importance are the following questions:

1. General information

- What type of app is the app in question?
- Does the app have an exact name?
- Is there an exact versioning of the app?
- Who is the vendor of the app?
- Could the app be installed successfully?
- Have, in addition to the app, other unrecognized installations of other apps or other software been carried out?
- Has the user given his/her consent?

2. Signing up options

- Is it possible to use the app without registration by mentioning personally identifiable information?
- Is the function delimited without registration?
- What other apps can the user log into / can be synched to the respective app?
- Can the user login with an e-mail address?
- Can the user change his data?
- Can the user delete his data?

II. Data Security

The app vendor must be able to show that, in his/her app, a sufficient amount of technical and organizational safety measures for the protection of personal data have been implemented. In this case, the following questions are of relevance:

1. Data traffic

- Is data traffic generated by the app?
- What types of data traffic are generated?
- Where does the data traffic (WHOIS) come from and where does it go?
- Is the user clarified about the scope of the data traffic in the data protection declaration?

2. Incoming and outgoing data

- Is incoming data encrypted?
- Will outgoing data be encrypted?
- Are the encryptions secure?
- Can encrypted, confidential data be decoded?

3. Use of tracking cookies

- Are tracking cookies made use of?
- Does the data protection declaration provide explanatory information about the tracking cookies?
- Do the cookies include personally identifiable information (e.g. IP address)?
- Do the cookies contain a time stamp?

4. Access to personal data

- Are the directories of the devices accessed (e.g. contact information, calendar, etc.)?
- Is exact location data accessed (e.g. GPS coordinates)?
- Is the device hardware accessed (e.g. microphone)?

5. Transfer of master data

- What device master data does the app access (e.g. IMEI, UDID, MAC, IP, IMEI)?
- How is this master data saved and stored by the app?

III. General principles of data protection

1. Principles of data reduction and data economy

The laws on data reduction and data economy must be taken into consideration (§3a of the Federal Data Protection Act). Thus, for the selection and design of the app, the principle of collecting, processing, and using as little personally identifiable information as possible must be taken into consideration.

- Is personally identifiable information collected and stored as part of using the app, and/or transferred to the app vendor? If so, is this to be done in an encrypted manner and must the deployed encryption technologies correspond with current standards?

- Will personally identifiable information, in as much as it is possible in accordance with the intended purposes and does not demand any excessive effort with respect to the intended protective purpose, be anonymized or pseudonymized as part of the usage of the app? If so, do the encryption technologies being made use of correspond to the current standards?

- Will only the personally identifiable information that is absolutely required for the intended purpose be collected or processed and used?

- Have sufficient measures been taken to keep the amount of data to be processed to an absolute minimum? If so, what measures?

- Is required data deleted immediately for every step of use and/or is data that is no longer necessary for the original processing purpose deleted immediately?

- How are the deletion or anonymization and pseudonymization of the data conducted?

- Will the anonymization or pseudonymization be conducted at the earliest possible point in time?

- Is it guaranteed, in the case of a pseudonymization of data, that this data can not be "depseudonymized" again without great efforts?

2. Transparency

Description of the app: The user must be provided with a clear comprehensible description of the product or service offered.

- Is the user provided with a clear comprehensible description of the product or service offered?

- Is the data processing flow as well as any data transfers or access rights sufficiently clear in this description? Are the notification obligations as defined in §§ 13 ff. TMG met?

3. Information obligations

The app must meet the following information obligations:

- Does the online product or service contain sufficient information to identify the supplier?
- Is there an imprint that corresponds with the requirements of §5 of the TMG?
- Has the user been sufficiently clarified, as part of a data protection declaration, in very clearly understandable wording, about the data processing, most especially about the type, scope, and purpose of the collection and usage of personally identifiable information?
- Is the informing about the data collection correct and complete?
- If the data is also processed outside of the EU/EEA: Is the user informed about this?
- If usage profiles are created: Is the user informed about this as well as his/her right of objection?
- Is a sufficient amount of information and explanation provided about cookies, weblogs, analysis or tracking services, etc.?
- Can the data protection declaration be called up at any time?
- Is the data protection explanation versionized?

As long as a data is transferred to another service provider takes place:

- Is the user shown this data transfer?
- Does this take place in an understandable manner?

4. Intended purpose and changes in purpose

During data storage, processing, and usage, the app vendor must ensure that the collected data is only processed as per its intended purpose or that of a legally permissible change in purpose is provided.

- Is it ensured that the collected data is only processed as per its intended purpose?
- Will the purpose for which the personally identifiable information is collected be documented?

5. Allowance of the data processing

Allowance of the collection, processing, and usage of personally identifiable information:

Personally identifiable information is only collected, processed or used, because either a law allows it to be or the affected parties have complied with this.

In as much as consent must be obtained from those affected, one must ensure that this consent is based on the freely made decision of those affected. In addition, when obtaining this consent, it must also be ensured that those affected have been informed of the consequences of refusing consent in addition to the intended purpose of the collection, processing or usage as well as in as much as it is required or requested in accordance with the circumstances of the individual case. The app vendor must also ensure that the consent has been obtained in the legally intended form.

- Is there a legal general permission for processing the data, e.g. as per the §§28 et seqq. of the Federal Data Protection Act or §§67a et seqq. of the Social Security Code (SGB X)?
- If this is not the case: Has the consent of the affected user been acquired in an effective manner?
- Is the formulation of a provided consent declaration sufficiently concrete, e.g. are the required specifications on the data-processing position, the type of data that is to be processed, planned transmission as well as the recipients of this eventual transmission, purpose of the data processing as well as also a reference to the revocability of this consent as well as their voluntariness?
- Are the normed formalities listed in §§ 4a of the Federal Data Protection Act, 12 et seqq. of the TMG being upheld? Has the consent been provided in the required form (§13 Par. 2 of the TMG), unless special circumstances require another form?
- Does the user data reach the app vendor? If so, has the user been informed about this as part of the installation?

6. Special categories of personal data

If the respective app vendor collects, processes or uses special categories of personal data in terms of §3, Par. 9 of the Federal Data Protection Act for individual business objectives, it has to be ensured that the prerequisites of the §28, Par. 6-9 of the Federal Data Protection Act are upheld.

- Especially sensible data as per §3, Par. 9, of the Federal Data Protection Act are specifications about the race and ethnic origin, political opinion, religious or philosophical persuasion, union affiliation, health or sexual life. In as much as these should be processed, the following demands apply:

- If the data collection and storage is for one's own business objectives in terms of §28 of the Federal Data Protection Act, the constraints of §28, Par. 6-9 of the Federal Data Protection Act must be considered.

- The data collection and storage of this very sensible data is permitted for one's own business objectives, should the affected party not have given its consent, when

    - this is required to protect the life-important interests of those affected or of a Third Party in as much as those affected are not able to give their consent for physical or legal reasons.

    - this is data that has been obviously been made public by those affected.

    - this is required so as to assert, exercise or defend legal claims and there is no reason to assume that the interests of those affected that are worthy of protection outweigh the exclusion of the collection, processing or usage.

    - this is required for conducting scientific research in which the scientific interest in conducting the planned research considerably outweighs the interest of those affected with respect to the collection, processing and usage, and that the purpose of the research is not assumed to another degree and can be achieved without a disproportionate amount of effort.

- The collecting of special categories of personal data is also permitted if it is required for the purpose of health care, medical diagnoses, tertiary-care or treatment, or for the administration of health services and the processing of this data through doctoral personnel or through other people who are subject to a respective obligation of secrecy.

- For another purpose, this very sensible data can only be transferred or used in accordance with the prerequisites described in §28, Par. 6, No. 1-4 and of §28, Par. 7, Sentence 1. In addition, a transmission or usage is also permitted if this should be necessary so as to ward off substantial dangers for state and public safety as well as for the persecution of very serious crimes.

7. Collection and processing von usage data as well as the creation of usage profiles

When calling up the app, the app vendor must ensure that only the usage data permitted by §15, Par. 1 of the TMG is collected. Should the app vendor usage profile be established under a pseudonym for the purpose of advertisement, market

research or adequate designing of telemedia, the app vendor must ensure that the requirements of §15, Par. 3 of the TMG are observed.

- Which usage data is collected?
- Who is collecting this usage data?
- Is this usage data also saved and stored? If so: By whom and for how long?
- When is the usage data deleted?
- Is only the usage data collected, which is required for the performance or billing of the offered service?
- Is it ensured that the usage data isn't processed for any other purpose?
- Is only the usage data stored that is required for billing the offered service?
- Is inventory data also collected?
- Should the IP address also be gathered: Who collects the IP address and for what purpose?
- Is the IP address also saved and stored? If so: For how long?
- If cookies are used:
    - What types of cookies are used?
    - Can the user contradict the setting of the cookies?
    - Is the data stored in the cookies read and sorted out? If so: Is this data stored? For what purpose?
    - Has user consent already been obtained?
    - Is there an option to declare an objection ("opt out") in terms of §15, Par. 3 of the TMG?
    - Should the analysis or tracking services be used: Are these safe concerning data protection? Is the user informed of this as part of the installation?

8. Guarantee of the rights of those affected

The app vendor must guarantee that the legally anchored rights of those affected can be enforced in an effective manner and that the technical and organizational

measures required for this are established. This especially includes, in reference to the data possibly stored by the app vendor, the following rights or obligations:

Right of information

- Is all the information that the user requires to let him/her assert his/her demand for information easy to find?
- Does the option for information correspond to the complete demand for information, thus to all data, all legal and purpose-related bases, origin, and recipient circle possibly stored by the app vendor?
- Is it sufficiently ensured in the case of information being demanded that the inquirer is authorized to confer the information?
- If this personally identifiable information is transmitted to the inquirer, does a logging of the transmission take place?

Rights of authorization of incorrect data

- As soon as the incorrectness of personally identifiable information is determined, is this data corrected immediately?
- Is there an automated authorization processing?
- Is it ensured that a recipient of previous data transmission is informed about this authorization?

Right to delete or block personally identifiable information

- Is personally identifiable information completely or irreversibly deleted by the app vendor?
- According to what time schedule is this data deleted?
- Is it certain that the now deleted data cannot be regenerated?
- Is it ensured that the deletions are sent to recipients of previously transmitted data?
- Should there be a blockage instead of the deletion of the data, because the deletion has an obstacle of some sort to face, it must be guaranteed that this stored personally identifiable information is pointed out so as to delimit its further processing or usage. Is there an option to mark the data records such that they remain stored, but are not used as part of the normal processing?
- Is this blockage guaranteed by a sufficient procedure?

- Is there a logging with respect to the point in time, but also to the contracting authority with respect to the blockage and particularly the collection of this blockage?

Rights of objection for those affected

- The user has the right to object to the collection, processing or usage of his/her data. Should there be an objection on behalf of those affected, the further processing of his/her personally identifiable information must be discontinued should the interests of those affected that are worth being protected outweigh the interest of the data-processing site due to his/her special personal situation.

- Is it guaranteed that an objection of this sort is immediately taken into consideration?

- Is it ensured that after the conducted objection, the corresponding data is immediately deleted?

- Is it ensured that such contradictions are also passed along to the recipient of previous data transmissions?

Obligation duty to transfer data and the duty to inform as of §6, Par. 2 of the Federal Data Protection Act

When several sites for the storage of a user's personal data are authorized, these sites are obligated to send any and all requests from a user to those sites which have actually stored the data. Going above and beyond this, the user must also be informed about this forwarding of this in advance and also about the respective site itself.

- If requests of this nature from those affected are submitted, it must be ensured that these are immediately passed along to the site that actually stored the data. Is this the case?

- Is it ensured that those affected as well as the respective site are immediately informed of this passing along of the request?

IV. Online Behavioral Advertising (OBA)

As part of self-regulation, companies across Europe have obligated themselves to establish transparency when using so-called behavior-based advertisement ("OBA") and to strengthen the self-determination of the consumers through simple to manage

decision mechanisms. For this purpose, the DDOW (German Data Protection Council for Online Advertisement) has developed guidelines (codices) that must be upheld by a participant of the self-regulation. OBA in terms of the codices is "...the collection and processing of data that is accrued over a specific period of time when visiting one or several websites with the goal of determining consumer interest preferences based on the collected data, in order to be able to deliver advertisement that could correspond with their preferences and interests". For all companies that operate OBA, it is mandatory that a clear and understandable reference be made to data collection and collection for OBA purposes on the individual websites.

The following questions must be answered:

1. General information

- Is, in the data protection declaration, information provided about the purpose for the OBA data processed, including information on whether and to whom such data can be transferred (data transfer to a Third Party)?
- Is information provided as to whether the app vendor is subject to the codex, and is a link to the DDOW pages provided?

2. Tracking

- Does a 1st Party Tracking of the user take place?
- Does a 3rd Party Tracking of the user take place?
- Is information provided about the tracking?
- Is there an option to opt out of the tracking?
- Does a reach measurement take place via the app?
- Is information provided about the reach measurement?
- Is there an option to opt out of the reach measurement?

3. AdMarker

- Is the AdMarker (icon, link) faded in for OBA advertisement?
- Is the user thoroughly informed about OBA when he/she clicks on the AdMarker?
- Is there an opt-out as part of the OBA framework?

4. Privacy Settings

- Are user-specific settings possible, e.g. for access to contact information, calendar information, media files, geographical data, etc.?
- How do these settings work?

Part B

Further requirements according to the EU General Data Protection Regulation ("GDPR"):

1. Principles relating to processing of personal data:

The principles relating to processing of personal data according to Art. 5 GDPR must be considered.

- Are personal data processed lawfully, fairly and in a transparent manner in relation to the data subject? Thus are the principles of lawfulness, fairness and transparency met?
- Are personal data collected for specified, explicit and legitimate purposes? Are they not further processed in a manner that is incompatible with those purposes?
- Are the collected personal data adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization')?
- Are personal data recorded accurate and, where necessary, kept up to date? Is every reasonable step taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')?
- Are personal data kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed?
- Are personal data processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality')?

2. Lawfulness of processing:

Is the processing lawful because:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

3. Change in purpose:

Are personal data proceeded for a purpose other than that for which the personal data have been collected? Is that based on the data subject's consent or on a Union or Member State law?

4. Lawfulness of the user's consent:

Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

If the data subject's consent is given in the context of a written declaration,

- Is the request for consent presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language?

- Is it assured that the data subject has the right to withdraw his or her consent at any time? Is it assured that it is as easy to withdraw consent as to give it? Is the concerned data subject prior to giving consent informed of his or her right of objection?

- Is the consent is freely given? Has been taken into account whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract?

- Is it assured that, in case of the processing of the personal data of a child, the child is at least 16 years old?

5. Processing of special categories of personal data:

If the applicant processes special categories of personal data, the requirements of Art. 9 GDPR have to be met.

Special categories of personal data are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Its processing is prohibited if none of the followings apply:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorized by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e) processing relates to personal data which are manifestly made public by the data subject;

f) processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;

g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in

accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

6. Upholding data subjects' rights and freedoms:

The applicant must guarantee that the data subjects' rights specified in Art. 12 ff. GDPR are assured. These are inter alia the following rights and obligations:

Transparent information, communication and modalities:

- Is the data subject provided with all information relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child?
- Is the information provided in writing, or by other means, including, where appropriate, by electronic means?
- Where personal data relating to a data subject are collected from the data subject, is the data subject provided with all of the following information:
    a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
    b) the contact details of the data protection officer, where applicable;
    c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
    d) where the processing is based on point (f) of Article 6(1) GDPR, the legitimate interests pursued by the controller or by a third party;
    e) the recipients or categories of recipients of the personal data, if any;
    f) where applicable, the fact that the controller intends to

transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1) GDPR, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

7. Right of access by the data subject:

Is ensured that the data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed (according to Art. 15 GDPR)?

8. Right to object:

According to Art. 21 GDPR, the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on points (e) or (f) of Article 6(1) GDPR.

- the right to object applies as well in case of profiling based on points (e) or (f) of Article 6(1).
- It has to be assured that the controller no longer processes the personal data in the event of an objection unless the controller demonstrates compelling legitimate grounds for the processing according to Art. 21(1) GDPR.
- Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
- It has to be ensured that where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
- It has to be ensured that at the latest at the time of the first communication with the data subject, the right to object is explicitly

brought to the attention of the data subject.

9. Security of processing:

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the applicant has to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk (according to Art. 32 GDPR).