ePrivacyseal GmbH

Criteria catalog 4.0.

September 05, 2024

The ePrivacyseal certifies for the respective applicant that its product or service is in line with the detailed criteria in the following criteria catalog based on the requirements of European data privacy law, in particular the applicable EU General Data Protection Regulation.

Note: The list of criteria has not yet been approved in accordance with Art. 42 para. 5 GDPR, as the relevant procedures have not yet been made available by the supervisory authorities. ePrivacyseal GmbH is therefore currently not an approved certification body within the meaning of Art. 42 para. 5 GDPR, as such an approval is currently not possible. As soon as a corresponding certification procedure is available, ePrivacyseal GmbH will submit the necessary applications. The applicants should not give any other impression.

I. General principles

1. Principles relating to processing of personal data

The principles relating to processing of personal data according to Art. 5 GDPR must be considered. When selecting and organizing the system, the primary objective must therefore be to collect, process and use as little personal data as possible.

- 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')?
- Is the personal data rendered anonymous or pseudonymized as allowed by the purpose for which it is collected as far as the effort required is not disproportionate to the desired purpose of protection?
- If personal data is collected, processed and used: has it been established in advance if it is possible to render said data anonymous or pseudonymize it?
- Is only the personal data collected, processed and used which is absolutely necessary for the intended purpose?
- Have sufficient measures been taken to keep the amount of data to be processed as low as possible? If so, which ones?

- Is the data which is no longer necessary for the original intended purpose deleted without delay at each processing step?
- How is the data deleted and/or rendered anonymous or pseudonymized?
- Is the data rendered anonymous or pseudonymized at the earliest possible moment?
- In the event that data is rendered anonymous is it ensured that this process cannot be reversed for this data with little effort?
- Have the employees been sufficiently trained with regards to the principles of data reduction and data economy?

2. Transparency

a) Description oft he product/service

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 this description always updated?
- Is the data processing flow sufficiently clear as well as any data transfers or access rights in this description?

b) Notification obligations

The applicant must meet the following notification obligations if the certification object is an online product or service:

- Enthält das Online-Angebot eine ausreichende Anbieterkennzeichnung?
- Is company information provided that includes all necessary details?
- Is commercial communication (i.e. advertising e.g. by email) clearly marked as such and is the company which sends said communication clearly identifiable?

- If offers to boost sales such as discounts, bonuses and gifts are offered, are these clearly recognizable for the user and are the conditions for their use easily accessible and clear and explicit?

- Are any contests and competitions of an advertising nature clearly identified as such and are their participation terms easily accessible and clearly explained?

- Are the identity of the sender and the commercial nature of the message clearly evident in advertising emails?

- Is the user, as part of a privacy policy, sufficiently informed in plain language about data processing, especially the type, scope and purpose of the collection and use of personal data?

- Is correct and complete information provided about the data collection?

- Is the user informed if the data is processed outside the EU/EEA?

- If user profiles are compiled, is the user made aware of his/her objection rights?

- Is sufficient information provided about cookies, weblogs, analysis and tracking services, etc.?

- Can the privacy policy be accessed at any time?

- If there is a reassignment to another service provider:

  - Is the user informed of this reassignment?

  - Does this happen in a way which is easy to understand?

3. Binding purpose and change of purpose

When storing, processing and using the data, the applicant must ensure that the data collected is only used for its intended purpose or that there has been a legally permissible change of purpose.

- Is it ensured that the data collected is only processed in accordance with the purpose intended?

- In connection with this, is the purpose for which the personal data is collected documented?

- Are data records marked with the corresponding purposes?

- Is a record kept of the processing of the data, in order to prove any change of purpose, if necessary?

4. Separation rule

The applicant must ensure that the separation rule is upheld during its data processing. The separation rule requires that data collected for different purposes can be processed separately from each other.

- If data from different sources is stored at a central location: Is it technically and organizationally guaranteed that individual data records can be read out solely on a purpose-related basis?

- If the applicant is an IT services provider: If there are several clients, is it guaranteed that the data processing systems are organized in such a way that the data areas of the clients do not accidentally overlap and as a result data belonging to one client can accidentally be read out by another client?

II. Lawfulness of data processing

1. Lawfulness oft he collection, processing and use of personal data

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.

2. Special categories of personal data

If the respective applicant collects processes or uses special types of personal data for its own commercial purposes as defined in Article 9 (1) of GDPR, it must in particular be ensured that the preconditions of Article 9 of GDPR are upheld.

Special categories of personal data pursuant to Article 9 (1) of GDPR are details about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life. If said data has to be processed the following requirements shall additionally apply:

- If special categories of personal data is processed and stored, the requirements of Art. 9 GDPR have to be met.

- The collection and storage of sensitive data for own business purposes is only permissible within the scope of the exceptions provided for in Art. 9 (2) of GDPR and if the data subject has not given effective consent, e.g.:

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 of GDPR;

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.

3. 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?

- Has consent been granted in the prescribed manner?

- Has this consent been made distinguishable in its appearance if it is given together with other written declarations?

- If consent should be granted through an electronic medium such as email or the Internet, this can also take place electronically.

- Are the consents collected/archived so that, on request, for each individual client the consent submitted can be retrieved as proof?

4. Cookies, TDDDG

- Is information stored in the end user's terminal equipment in accordance with Section 25 (1) TDDDG ? If yes, is consent obtained?

- Is information accessed in the end user's terminal equipment in accordance with Section 25 (1) TDDDG ? If yes, is consent obtained ?

- Is the consent according to § 25 para. 1 TDDDG is **not** required,

  because the sole purpose of storing information in the end user's terminal equipment or the sole purpose of accessing information already stored in the end user's terminal equipment is to carry out the transmission of a message over a public telecommunications network;

  because the storage of information in the end user's terminal equipment or the access to information already stored in the end user's terminal equipment is strictly necessary for the provider of a telemedia service to provide a telemedia service explicitly requested by the user ?

5. Guaranteeing the data subject's rights

The applicant must guarantee that the data subjects' rights specified in Art. 12 ff. GDPR are assured and processes to guarantee these rights are documented.

- 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.

- Are, in addition to the above-mentioned information, at the time when personal data are obtained, the following further information provided, that are necessary to ensure fair and transparent processing:

    a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

    b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing

concerning the data subject or to object to processing as well as the right to data portability;

c) where the processing is based on point (a) of Article 6 (1) or point (a) of Article 9 (2) GDPR, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

d) the right to lodge a complaint with a supervisory authority;

e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

- Is ensured that, where the applicant intends to further process the personal data for a purpose other than that for which the personal data were collected, the data subject is provided with information on that other purpose?

6. Right of access

- 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)? And where that is the case, is his or her access to the personal data and the following information guaranteed:

  - the purposes of the processing;

  - the categories of personal data concerned;

  - the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;

  - where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

- the right to lodge a complaint with a supervisory authority;

- where the personal data are not collected from the data subject, any available information as to their source;

- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

- the existence of a right of appeal to a supervisory authority.

- Is all the information which the user needs to satisfy his/her right to be informed easy to find?

- Can the user receive information meeting his/her right to be informed in full, in other words information about data stored, the purpose of storing said data and its legal basis, the origin and group of recipients?

- When information is requested, is it sufficiently ensured that the enquirer is entitled to receive the information?

- When this personal data is provided to the enquirer, is a record kept of the transfer of information?

7. Right to rectification

According to Art. 16 GDPR, the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

- As soon as it is ascertained that personal data is inaccurate, is it rectified without delay?

- Is there an automated rectification process?
- Is it ensured that recipients of prior data transfers are informed about this rectification?

8. Right to deletion and blocking of personal data

- Is guaranteed that the data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay (according to Art. 17 GDPR) and that the controller has the obligation to erase personal data without undue delay where one of the following grounds applies:

    a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

    b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2) GDPR, and where there is no other legal ground for the processing;

    c) the data subject objects to the processing pursuant to Article 21(1) GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) GDPR;

    d) the personal data have been unlawfully processed;

    e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

    f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1) GDPR.

    This will not apply only if the conditions of Art. 17(3) GDPR are satisfied.

- Is personal data completely and irreversibly deleted?
- After which time period is this data deleted?
- Is it ensured that data which was originally deleted cannot be restored again?
- Is it ensured that these deletions are passed on to recipients who have received this data in the past?

- If in place of the data being deleted it is blocked because there is an impediment to the deletion, it must be guaranteed that this personal data stored is marked to limit its further processing or use. Is there a possibility of marking the data records in such a way that they remain stored but cannot be used in the course of the standard processing?
- Is this blockage guaranteed by a sufficient procedure?
- Is a record kept of the time that the blockage occurs and who places the order and if the blockage is reversed?

9. Right to restriction of processing

It must be guaranteed that the data subject has the right to obtain from the controller restriction of processing according to Art. 18 GDPR where one of the following applies:

a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims;

d) the data subject has objected to processing pursuant to Article 21(1) GDPR pending the verification whether the legitimate grounds of the controller override those of the data subject.

10. Right to data portability

It must be guaranteed that the data subject has the right and can enforce the right to data portability according to Art. 20 GDPR.

11. 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.

The user has the right to object to the collection, processing or use of his/her data. Following an objection by the data subject, there must be no further processing of his/her user data if the interests of the data subject worthy of protection due to his/her particular situation outweighs the interests of the data processing body.

- Is it guaranteed that this type of objection is considered without delay?

- Is it guaranteed that once the objection has been lodged the corresponding data shall be irrevocably deleted?

- Is it ensured that objections of this type are also passed on to previous recipients of data transmissions?

12. Automated individual decision-making, including profiling

It must be assured that the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her according to Art. 22 GDPR. This right shall not apply if the decision:

a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

b) is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

c) is based on the data subject's explicit consent.

In the cases referred to above, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. Decisions referred to above shall not be based on special categories of personal data, unless point (a) or (g) of Article 9(2) GDPR apply.

13. Right to be informed about forwarding of enquiries

If more than one body is entitled to save the personal data of a user, these bodies undertake to pass on any enquiries of a user to the body that has actually stored the data. Additionally, the user shall also be informed about the forwarding of such enquiries and of the body responsible.

- If these types of enquiries are received from a data subject, it must be ensured that they are forwarded without delay to the body which has actually stored the data. Is this the case?

- Is it ensured that the data subject is promptly informed that the enquiry has been forwarded and to which body it has been forwarded?

III. Data privacy management

The overall organization of the applicant takes into account the interests of data privacy so that sufficient standards and provisions are in place to guarantee the data privacy goals are met.

Applicants and processors must not only produce the safety measures required of them once, but must also ensure their safety "in the long term". They must also regularly subject their effectiveness to a critical review by means of suitable procedures.

1. Records of processing activities

It must be ensured that the applicant maintains a record of all processing activities under its responsibility. That record shall contain in particular the following information:

a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

b) the purposes of the processing;

c) a description of the categories of data subjects and of the categories of personal data;

d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations;

e) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1) GDPR, the documentation of appropriate safeguards;

f) where possible, the envisaged time limits for erasure of the different categories of data;

g) where possible, a general description of the technical and organizational security measures referred to in Article 32(1) GDPR.

Furthermore, it has to be ensured that each processor and, where applicable, the processor's representative maintains a record of all categories of processing activities carried out on behalf of a controller, containing:

a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

b) the categories of processing carried out on behalf of each controller;

c) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1) GDPR, the documentation of appropriate safeguards;

d) where possible, a general description of the technical and organizational security measures referred to in Article 32(1) GDPR.

Every record has to be in writing, including in electronic form. The above mentioned obligations shall not apply to an enterprise or an organization employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data.

2. Order processing

If necessary, the applicant must conclude commissioned data processing agreements.

- Is data being processed by third parties?
- Is this type of data processing by a third party permissible?
- Has a corresponding commissioned data processing agreement been concluded?
- Have the details to be specified pursuant been determined regarding the agreement?
- Are there sufficient technical and organizational measures which in particular also guarantee that the contractor follows the instructions of the body responsible?

- Has compliance with the sufficient technical and organizational measures been monitored and have the results of the inspection been documented?

Where processing is to be carried out on behalf of a controller, the controller must ensure to use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

It has to be assured that the processor does not engage another processor without prior specific or general written authorization of the controller.

Processing by a processor must be governed by a contract or other legal act according to Art. 28(3) GDPR, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

That contract or other legal act shall stipulate, in particular, that the processor:

a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

b) ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c) takes all measures required pursuant to Article 32 GDPR;

d) respects the conditions referred to in paragraphs 2 and 4 of Art. 28 GDPR for engaging another processor;

e) taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to above shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of this Regulation.

3. Technical and organizational security measures

The applicant must demonstrate that sufficient technical and organizational security measures have been implemented in its company in the sense of Article 32 GDPR. Such measures are only necessary if the effort required is in reasonable proportion to the desired purpose of protection.

As a wide range of different formulations are possible in order to reach the minimum standard, the following questions are solely provided as an indication or example of what is needed to meet these minimum requirements.

a) Access checks

Unauthorized persons must be prohibited from accessing data processing systems with which personal data is used or processed, whereby the term is to be understood spatially.

- Access inspection system, ID card reader, magnetic card, chip card
- Key/key allocation

- Door security (electrical door opener etc.)
- Plant security, desk officer
- Surveillance system such as alarm system, video/television monitor

b) Access control

The intrusion/use of unauthorized persons into/of data processing systems must be prohibited through technical (password/code protection) and organizational (user master record) measures regarding user identification and authentication.

- Password procedures (i.e. special characters, minimum length, regular change of the code word)
- Automatic blockage (e.g. password or pause protection)
- Access to the server only with a personal account and specially defined access rights (user groups)
- Setting up a user master record per user
- Encrypting data carriers and/or data traffic between the servers
- Issuing admin accounts
- Only authorized persons have access to the server systems

c) Admission control

Unauthorized work in data processing systems outside the rights granted must be prohibited by rights only being granted when needed and these rights being closely monitored and logged.

- Differentiated rights (profiles, roles, transactions and objects), e.g. through managing rights and access control
- Setting up a user administration system
- User and rights management only by clearly defined IT employees
- Use of professional and safe archiving systems
- Reliable deletion of data and data carriers

d) Transfer control

The aspects of the transfer of personal data must be regulated for example regarding the electronic transfer, data transport, transfer checks, etc. These also include measures when transporting, transferring and circulating or saving to storage media (manually or electronically) as well as the subsequent inspection.

- Securing the electronic communication paths, e.g. by setting up closed networks or procedures to encode data to be transferred
- Tunnel connection (VPN = Virtual Private Network)
- Electronic signature
- Logging
- Transport security, e.g. by using safe transport containers for data carriers

e) Input control

The traceability and documentation of the data administration and maintenance must be guaranteed e.g. through measures to subsequently check if and by whom data has been entered, changed or removed (deleted).

- Detailed logging and logging evaluation systems with regard to the creation, modification and deletion of data records

f) Job control

If data is processed on behalf of others under Article 28 of GDPR it must be ensured that the data processing is carried out in line with instructions by having measures in place (technical as well as organizational) which define the responsibilities of the client and the contractor.

- Clear contractual formulation
- Formalized and thus standardized allocation of contracts (order form) and instructions
- Criteria for selecting a contractor
- Clear delineation of responsibilities
- Control of the contract management

g) Availability control

The data must be protected against accidental destruction or loss through physical and logistical measures for data backup.

- Backup procedure
- Mirroring hard disks, e.g. RAID
- Regularly compiling full backup copies and storing them in another location
- Regularly testing the data reconstruction
- Uninterrupted power supply (battery run)
- Anti-virus protection/firewall
- Generating an emergency concept and corresponding written documents

h) Purpose control

Data which was collected for different purposes must be processed separately. Therefore, measures must be guaranteed for the separate processing (storing, modification, deletion, transfer) of data with different purposes.

- Issue of access rights/restrictions
- Encoded storage of personal data, so that if it is accidentally accessed by third parties it cannot be read
- Storage on physically separate systems (separation according to skills and areas of responsibility)

4. Incident response management

In case of a breach of personal data, the applicant is obliged (Art. 33 of GDPR) to report the breach to the supervisory authority in accordance with Article 55 without delay and if possible within 72 hours of becoming aware of it, unless the breach of the protection of personal data is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by a justification for the delay.

5. Data protection by design and by default

The applicant shall take appropriate technical and organizational measures to ensure that, by default, only personal data whose processing is necessary for the respective specific processing purpose will be processed. The person responsible must therefore design his or her default settings, especially for online and telemedia, in such a way that only the data required for the respective processing purpose is processed.

This obligation applies to the amount of personal data collected, the scope of its processing, its storage period and its accessibility. In particular, such measures must ensure that personal data are not made available to an indefinite number of natural persons by default without the intervention of the person.

6. Internal regulations

The applicant must explain that his or her company has sufficient internal regulations, especially for employees, on the subject of data protection.

- Have all employees involved in data processing been obligated to data secrecy?
- Are there systematic regulations in the companies regarding the handling of personal data?
- Are there instructions available for employees on questions arising in the area of data protection?
- Are employees regularly made aware of the issue of data protection or are appropriate training courses held at regular intervals?

7. Data protection impact assessment

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data according to Art. 35 GDPR. A single assessment may address a set of similar processing operations that present similar high risks. A data protection impact assessment shall in particular be required in the case of:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

b) processing on a large scale of special categories of data referred to in Article 9(1) GDPR, or of personal data relating to criminal convictions and offences referred to in Article 10 GDPR; or

c) a systematic monitoring of a publicly accessible area on a large scale.

The assessment shall contain at least:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Data protection officer

The applicant has to designate a data protection officer in any case where:

a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10 GDPR.

The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39 GDPR.

The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

9. Transfer of personal data to third countries or other international organizations

It must be ensured that any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization take place only if the conditions laid down in Art. 44 GDPR are complied with by the controller and processor.

A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection. Such a transfer shall not require any specific authorization.

In the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

The appropriate safeguards may be provided for by:

a) a legally binding and enforceable instrument between public authorities or bodies;

b) binding corporate rules in accordance with Article 47 GDPR;

c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2) GDPR;

d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2) GDPR;

e) an approved code of conduct pursuant to Article 40 GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

f) an approved certification mechanism pursuant to Article 42 GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

Subject to the authorization from the competent supervisory authority, the appropriate safeguards may also be provided for, in particular, by:

a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organization; or

b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

The transfer may be carried out based on Binding corporate rules according to Art. 47 GDPR. The exceptions according to Art. 49 GDPR have to be taken into account.

It should also be taken into account that the European Commission issued new standard contractual clauses in June 2021 (Implementing Decision (EU) 2021/914 of the EU Commission dated 04.06.2021 - Ref. C (2021) 3972, OJ EU No. L 199/31 of 07.06.2021). The new standard contractual clauses are modular and can be used in the following constellations:

- Responsible party to responsible party
- Responsible party to processor
- Processor to (sub)processor
- Retransmission of the processor in the EU to a controller in the third country

The new standard contractual clauses have been mandatory for new contracts since September 27, 2021. All old contracts must be converted to the new standard contractual clauses by December 27, 2022 at the latest. In this respect, the advice of the LfDI and determination of its further course of action regarding the judgment of the European Court of Justice (ECJ) of July 16, 2020, Case C-311/18 ("Schrems II") must be taken into account in particular.

The following criteria are to be reviewed:

Is it ensured that the controller and processor only transfer personal data that are already being processed or are to be processed after their transfer to a third country or an international organization under the conditions laid down in Art. 44 DSGVO ?

Is the transfer of data based on an adequacy decision of the EU Commission within the meaning of Art. 45 GDPR ?

For the transfer on the basis of an adequacy decision, there must also be a contingency plan in the event that the decision is revoked. Is such a contingency plan available?

If there is no Commission Decision pursuant to Art. 45 III GDPR on an adequate level of protection for a third country or an international organization, a controller or a processor may only transfer personal data to a third country or an international organization if the controller or processor has provided appropriate safeguards and if enforceable rights and effective remedies are available to the data subjects. The safeguards may consist of:

- a legally binding and enforceable document between public authorities or public bodies

- Binding internal data protection rules pursuant to Article 47 GDPR.

- standard data protection clauses adopted by the Commission in accordance with the examination procedure under Article 93(2) GDPR.

If the clauses are used: does an assessment take place prior to the transfer of personal data as to whether a level of protection for personal data equivalent to that in the EU exists in the third country.

If so, additional measures may need to be taken to ensure a level of protection substantially equivalent to that in the EU, or the transfer may need to be refrained from. Have appropriate measures been taken ?

- standard data protection clauses adopted by a supervisory authority and approved by the Commission in accordance with the examination procedure referred to in Article 93(2) of the GDPR

- approved codes of conduct pursuant to Article 40 GDPR together with legally binding and enforceable commitments by the controller or processor in the

third country to apply the appropriate safeguards, including in relation to the rights of data subjects

- an approved certification mechanism pursuant to Article 42 GDPR together with legally binding and enforceable commitments by the controller or processor in the third country to apply the appropriate safeguards, including in relation to the rights of data subjects.

Subject to approval by the competent supervisory authority, such appropriate safeguards may also consist in particular of:

- Contractual clauses agreed between the controller or processor and the controller, processor, or recipient of the personal data in the third country or international organization

- Provisions to be included in administrative agreements between public authorities or public bodies that include enforceable and effective rights for data subjects.

A transfer may also take place on the basis of binding internal data protection rules pursuant to Art. 47 DSGVO. The exceptions pursuant to Art. 49 GDPR must be taken into account.

IV. OBA Framework

If the applicant engages in Online Behavioral Advertising („OBA") and also is a signatory of the IAB Europe EU Framework for Online Behavioral Advertising ("OBA Framework"), he also must be in line with the following criteria, based on the requirements of the OBA Framework.

1. Information requirement

The applicant that engages in OBA must provide the following information:

a) General information requirement

The applicant must provide the users and companies with easy accessible information about OBA, in particular about how data for OBA purposes is obtained, how it is used and how the user may exercise his user choice.

- Does the applicant's website provide information about its OBA business practices?
- Does this information contain at least the following descriptions:
  - What does OBA mean and how does it work?
  - How does the applicant use OBA?
  - How is the data for OBA purposes collected, stored and processed?
  - How may the user exercise his or her user choice?
- Is this information easily accessible for the user, e.g. by providing a clearly visible link on the website?
- Is the information provided in a simple language that the average internet user can easily understand?

b) Users' notice

If the applicant is an entity that engages in OBA on a website or websites other than a website or websites it or an entity which belongs to the applicant's group of companies owns or operates (so-called "Third Party"), the following information must also be provided:

a. Third Party Notice

On its website, the applicant must give clear and comprehensible information in simple layman's language on how the data for OBA purposes is collected and used.

Such notice should be provided under a clear link on its homepage and be distinct from the "Terms and Conditions" section.

In particular, the following information must be provided:

- applicant's name and contact information
- The types of data collected and used for OBA purposes, including an indication whether any data is personal data or special categories of personal data as defined by Art. 9 (1) of GDPR.
- The purpose or purposes for which OBA data is processed and the recipients or categories of recipients to whom such data might be disclosed.
- Information about an easy to use mechanism for exercising choice with regard to the collection and use of data for OBA purposes and a link to a website where such choice may be exercised, e.g. the OBA User Choice Website or a similar website.
- The fact that the applicant is a signatory of the OBA Framework and adheres to its principles.

b. Enhanced Notice

In addition, the applicant must also provide enhanced notice of the collection and use of data for OBA purposes in order to identify OBA (so-called "Enhanced Notice"):

- A standardized icon or pictogram (so-called „Ad Marker") in or around the advertisement which includes a link to the OBA User Choice Website or a similar website.

c) Information Requirements for Website Operators

If the applicant is a Web Site Operator who permits data to be collected from and used on a web site for OBA purposes by Third Parties, the applicant must disclose this arrangement as follows:

- A link that refers the user to an information page with at least the following information:

- List of Third Parties used by the website with which the user may interact;

- Links to further information related to OBA, e.g. the OBA User Choice website or similar websites;

- The link should be clear and available on all subpages, and distinct by the "Terms and Conditions" link.

2. Mechanism to Exercise User Choice

If the applicant is a so-called Third Party, he must also make available a mechanism for users to exercise their choice with respect to the collection and use of data for UBA purposes and the transfer of such data to Third Parties for OBA.

- There must be a clear link from the Ad Marker or the interstitial page to the website where the mechanism to exercise user choice is made available, e.g. to the OBA User Choice Website or a similar website.

- The integration of the applicant with the OBA User Choice Website or a similar website must be in place. If the integration mechanism fails for more than 5 % of the requests to turn off OBA over a period of one month, the applicant is deemed to be non-compliant with this criterion.

- The applicant must not use any technologies to circumvent the user‘s express choices.

3. Explicit Consent of the User / Mechanism to Withdraw

In the following cases, the applicant must obtain the user’s Explicit Consent:

a) Use of Specific Technologies or Practices

If the applicant collects and uses data via specific technologies or practices that are intended to harvest data from all or substantially all URLs traversed by a particular computer or device across multiple web domains and use such data for OBA, it must first obtain the user’s Explicit Consent.

b) Sensitive Segmentation

If the applicant seeks to create or use OBA segments relying on the use of special categories of personal data as defined in Article 8 (1) of Directive 95/46/EC, it must first obtain the user‘s Explicit Consent.

c) Requirements for a Valid Explicit Consent

For a prior Explicit Consent to be deemed valid, the following conditions must be met:

- The user must have been informed, with simple language easy to understand, that all or most of their browser activities will be collected and stored, in order to be later used for OBA purposes.
- Explicit Consent must be given specifically for collection and use of data for OBA purposes.
- Explicit Consent must be freely given, i.e. it must not be induced in any way, e.g. by suggesting users that certain functionalities would not be available if consent is not given.
- When obtaining Explicit Consent, the applicant must clearly inform the user that Explicit Consent can be withdrawn at any time and provide the user with a link to the withdrawal mechanism.

d) Mechanism to Withdraw

The applicant must provide the users who have given Explicit Consent with an easy to use mechanism to withdraw their Explicit Consent to the collection and use of OBA data:

- The applicant's website must include a clear, explicit link to the mechanism to withdraw, i.e. not in the Terms and Conditions or a similar link.
- The mechanism to withdraw must be simple and easy to understand and should not ask users for any additional data.
- Once the user has withdrawn the Explicit Consent, the applicant must not collect or use any further OBA data.

4. No Children's segmentation

The applicant must not create segments for OBA purposes that are specifically designed to target children (12 years or younger).

5. Complaints Handling

The applicant must ensure that user complaints about incidents of alleged non-compliance with the OBA Framework will be handled timely and satisfactory manner.

- The applicant must implement an easily accessible mechanism for complaints to be submitted directly to the applicant, e.g. by providing a complaints form on the applicant's website.
- Information about the steps undertaken and the time frame for dealing with the complaint must also be given.
- A user's complaint should be addressed within 7 business days.