Data protection requirements (privacy by design / privacy by default)

Contractual services must be designed, produced and configured in accordance with the principles of privacy by design (data protection through technology) and privacy by default (data protection-friendly pre-settings). Service providers must ensure and guarantee to the client that the data protection principles of Article 5(1) of the General Data Protection Regulation (GDPR) and the data protection specifications of Art. 25 GDPR are or can be complied with during the development, use, installation and/or resale of any developments.

Existing standards, methods and best practices must duly be taken into account. To this end, the data protection requirements specified in the “Controls” annex are applied to developments. The service provider must document the implementation of these requirements and, if required, make this documentation available to the client for the purpose of providing proof (accountability, Art. 5(2) GDPR).

The service provider must supply the client with sufficient information and, if necessary, configuration options to enable all parties involved in the development to meet their respective data protection obligations (such as accountability, obligation to erasure and information obligations) vis-à-vis business partners, authorities and data subjects and fulfill the data protection-related demands of the data subjects.

“Controls” annex

The following controls must form the basis of the designing of contractual services. Each of these controls must be refined further in a project- and product-specific manner within the framework of the development, and documented regarding its implementation. Example applications are included in the template for each control.

Please derive appropriate hardware, software and other development-specific requirements for each control, and describe these requirements and their implementation.

“Test questions on basic systemic conditions” are also assigned to the controls. These questions provide pointers on whether the planned hardware, software or other developmental results meet the basic technical conditions for implementing the relevant statutory requirements. The test questions on specialist procedural connections provide pointers about whether key specialist data protection-related requirements for technical implementation are known and have been implemented.

The “test questions on basic systemic conditions” are not part of the formal binding data-protection requirements.

The following requirements are derived from European Union data-protection legislation, especially the GDPR. Please note that, depending on the use or target market of the relevant hardware, software or other development results, different or additional requirements may apply, especially where these arise out of national legislation in the relevant country.

No.	Control	Description	Test questions on basic systemic conditions [Not a formal and binding part of the statutory requirements]	Test questions on specialist procedural connections
1	**Data minimization**	Data may be processed only to the extent necessary and appropriate for the relevant processing purpose. Data processing must be limited to what is necessary for the purpose in question.	Can the hardware, software or other development results delete data? (Deleted data must be removed permanently and irreversibly from the hardware, software or other development results in full, overwritten, and subsequently and securely anonymized.) Can the hardware, software or other development results block data (i.e. restrict access and prevent further processing)?	Are specialist deletion concepts in line with the deletion concept process available for the processing activities undertaken with the hardware, software or other development results? Have these been consolidated into a deletion concept? Has a technical deletion concept been derived and implemented?
2	**Transparency**	Data must be processed in an understandable way for the data subject. Information and notifications about the processing must be easily accessible and comprehensible for the data subject.	In the case of hardware, software or other development results with a user interface for data subjects: Do the hardware, software or other development results offer an opportunity to display and manage information/icons on data	Are any data protection notes that are required for implementation as well as further data protection information available pursuant to the specialist specifications as per the data protection note process?

			protection at an easily accessible location (e.g., within two clicks)?	Have these requirements been consolidated for the hardware, software or other development results? Have specialist implementation requirements been derived and implemented?
3	**Integrity and confidentiality**	Data may be processed only in a manner that guarantees adequate security. This includes protection against unlawful and unauthorized processing as well as accidental loss, destruction and damage.	Has the implementation of the necessary IT security requirements been verifiably confirmed for the hardware, software or other development results?	Were the necessary IT security processes conducted for the present hardware, software or other development results? In particular, is there an approved security concept?
4	**Purpose limitation**	The purposes of data processing must be explicit, legitimate, and already specified at the time of data collection.	Can the hardware, software or other development results manage rights and interfaces individually, and restrict them at any time? Can the hardware, software or other development results physically or at least logically separate clients	Are specialist rights concepts available for the processing activities undertaken with the hardware, software or other development results?

			from one another (client separation)?	Have these been consolidated into a rights concept? Has a technical deletion concept been derived and implemented?
5	**Data accuracy**	Processed data must be accurate and up to date. Inaccurate data must immediately be deleted or corrected.	Can the hardware, software or other development results modify (e.g. overwrite) data fields containing personal data? Can the hardware, software or other development results delete data? (Deleted data must be removed permanently and irreversibly from the hardware, software or other development results in full, overwritten, and subsequently and securely anonymized.) Can the hardware, software or other development results block data (i.e. restrict access and prevent further processing)?	
6	**Storage limitation**	Data must be stored in a form that permits identification of the data subject only for as long as this is necessary for the purpose of processing.	Can the hardware, software or other development results delete data? (Deleted data must be removed permanently and irreversibly from the	Are specialist blocking, pseudonymization and anonymization requirements* in place for the processing activities undertaken with the hardware,

			hardware, software or other development results in full, overwritten, and subsequently and securely anonymized so that no connection can be established to a natural person, even in combination with other data.) Can the hardware, software or other development results block data (i.e. restrict access and prevent further processing)? Can the hardware, software or other development results pseudonymize data (i.e. remove the name and replace it with a pseudonym)?	software or other development results? Have these been consolidated into development-specific requirements?* Have technical blocking, pseudonymization and anonymization requirements been derived and implemented? * (* The specialist requirements and technical implementation are implemented, for example, within the framework of the deletion concept, cf. the deletion concept process)
7	**Lawfulness of processing**	Personal data may be processed only if there is a statutory basis for this.	Only in the case of hardware, software or other development results with a user interface for data subjects: Can the hardware, software or other development results display and manage declarations of consent (e.g. one-click, by e-mail)? • If so, is consent NOT activated by default?	Are requirements regarding the technical implementation of consent and revocation mechanisms in place for the processing activities undertaken with the hardware, software or other development results? Have these been consolidated into

			• If so, is revocation as easy as providing consent (e.g. one-click, by e-mail)?	development-specific requirements? Have technical implementation requirements been derived and implemented? Are any declarations of consent that are required for implementation as well as further data protection information available pursuant to the specialist specifications as per the data protection note process, and have they been implemented?
8	**Rights of data subjects**	Care must be taken to ensure that data subjects can exercise the following rights regarding their data: Information/copy Rectification Erasure Restriction of processing Data portability Right to object	Can the hardware, software or other development results export all data fields into a standard data format, e.g. Excel, CSV, XML or PDF? Can the hardware, software or other development results modify (e.g. overwrite) data fields containing personal data? Can the hardware, software or other development results delete data? (Deleted data must be removed	Are specialist data subject rights concepts in line with the data subject rights concept process available for the processing activities undertaken with the hardware, software or other development results? Have these been consolidated into development-specific data subject rights concepts?

			permanently and irreversibly from the hardware, software or other development results in full, overwritten, and subsequently and securely anonymized so that no connection can be established to a natural person, even in combination with other data.) Can the hardware, software or other development results block data (i.e. restrict access and prevent further processing)? Can the hardware, software or other development results pseudonymize data (i.e. remove the name and replace it with a pseudonym)?	Have technical data subject rights concepts been derived and implemented?
9	**Good faith**	The processing of personal data may not be undertaken through exploitation of an unequal power relationship between the data controller and the data subject or as a result of unreasonable pressure on the data subject, and must be based on the principle of fairness and loyalty.		