Compact check list for the implementation of the General Data Protection Regulation

(VO [EU] 2016/679)

Version: 2.0
Status: September 2017

Legal notice Media owner, editor and producer: Austrian Association of operational and governmental data protection officers - Privacyoffiicers.at, ZVR-number (Central Associations register) 061847005, Vienna, https://www.privacyofficers.at/impressum

Preface of the Executive Board of the Association

Dear reader,

The Austrian Association of operational and governmental data protection officers Privacyofficers.at is pleased to be able to provide this compact check list in a revised version. Our goal is to keep this implementation help up-to-date. In the present version the Austrian Data Protection Amendment Act 2018 has been incorporated accordingly.

Special thanks for the elaboration are due to our study group data security and all association members involved. Based on the slogan "from members for members (and beyond)", a clearly arranged practical assistance has formed in short time.

The present check list is divided into three phases and describes the most important contents of the DSGVO (General Data Protection Regulation). With this check list you are provided a guideline to initiate compliance of your organization with the DSGVO and to keep the overview on your implementation project.

We may point out that this check list only summarizes the most important contents of the DSGVO in compact and clearly arranged form and does not claim comprehensive consideration of all provisions of the DSGVO, resp. of the national data protection provisions. The terms used in the present document correspond to the definitions as used in the DSGVO. Abbreviations are defined in the section "Abbreviations".

Privacyofficers.at hopes that the present check list will support many persons in charge and data processing companies with the implementation of the DSGVO, we have therefore subjected it to a CC BY-NC-SA 4.0 licence. We are happy to receive suggestions and positive critical comments under office@privacyofficers.at, current data protection news can be viewed on our website: https://www.privacyofficers.at/.

Executive Board of the Association

Abbreviations

- **BMI:** Austrian Federal Ministry of the Interior
- **BSI IT-Basic Protection:** The IT basic protection developed by the German Federal Office for security in information technology facilitates the identification and implementation of necessary security measures.
- **CERT:** A Computer Emergency Response Team (CERT: German „Computersicherheits-Ereignis- und Reaktionsteam“) is a group of EDV-security experts who operates as a coordinator in the solution of IT-security cases, resp. who deals with computer security in general.
- **CISO:** Chief Information Security Officer
- **DSB:** Data Protection Officer
- **DSG:** Federal Act for the protection of individuals with the processing of personal data (Data Protection Act - DSG) as amended in BGBl (Federal Law Gazette) I 120/2017
- **DSGVO:** Regulation (EU) 2016/679 of the European Parliament and the Council of April 27, 2016 regarding the protection of individuals with the processing of personal data, for free data traffic and for the cancellation of Directive 95/46/EG (General Data Protection Regulation), ABl L 119 dated May 4, 2016, 1-88, LINK to the full version including correction as of November 22, 2016).
- **DSMS:** Data Protection-Management System
- **FMA:** Financial market supervision
- **ISMS according to ISO/IEC 27001:** An information security management system is a schedule of procedures and rules to govern, control, maintain and continuously improve information security. The internationally acknowledged standard ISO/IEC 27001 specifies the requirements for the institution, implementation and maintenance of a documented ISMS.
- **ISO/IEC 31000:** International standard “Risk Management - Principles and Guidelines” which integrates risk management into all company activities
- **ITIL**: The IT Infrastructure Library (ITIL) is a collection of pre-defined processes, functions and roles as they typically occur in the IT infrastructure of medium-sized and big enterprises
- **KVP:** Continuous improvement process
- **NIS-Directive:** Directive (EU) 2016/1148 of the European Parliament and the Council as of July 6, 2016 on the measures for provision of a high common security level of network- and information systems within the European Union, ABl 194 as of July 19, 2016, 1-30 (LINK to the full version)
- **pb Data:** Personal data (see definition in Art 4 Z 1 DSGVO)
- **RTR:** The regulatory authority for radio- and telecommunication supports the Austrian Communications Authority as well as the Telecom-Control Commission with the performance of their tasks as their office and assumes various duties particularly in the fields of telecommunication and media
- **TOM**: Technical and Organisational Measure for the fulfilment of security- and protection measures
- **Procedure index:** Index of processing activities according to Art. 30 DSGVO

Table of contents

Phase 1: Preparation

1.1 Establish Management Awareness	in preparation ☐ done ☐
Description	The management shall be made aware of the data protection issue, because management support is mandatory for a successful implementation of the DSGVO.
Objective	• Create awareness in the management that the implementation of DSGVO-content offers versatile added value such as e.g. positive reputation, increased market chances etc. • Reduce liability risks in case of infringements
Activities	• Awareness event with the management • Delineation of content and necessary measures for data protection according to this check list • Proposal for the implementation of a DSMS • Illustration of synergy possibilities (ISMS according to ISO/IEC 27001, DSMS, NIS-Directive, ITIL etc.)
References	• Art. 5 para 2, 24, 82 and 83 DSGVO • §§ 4, 62 and 63 DSG • NIS-Directive • ISO/IEC 27001

1.2 Obtain project order for implementation project (secure management commitment)	in preparation ☐ done ☐
Description	A project order is prerequisite for the official start of each project. It may be qualified as an agreement between project manager and project principal. The cooperation as well as the clear definition of goals should be included in the project order.
Objective	• Establishment of a binding agreement between all parties concerned and definition of project content • Create information basis for team members entering at a later stage • Obtain management commitment
Activities	• Determine the project targets • What may/should NOT happen? (Non-targets) • Project phases and work packages • Milestones • Determine start and closing date (Timeline) • Determine project team and budget • Identify framework conditions which cannot be influenced • Identify critical success factors • Signature project manager and project principal
References	• Art. 5 para 2, 24 DSGVO

1.3 Provide necessary resources	in preparation ☐ done ☐
Description	The organisation shall determine and provide resources to establish, maintain and subsequently optimize the DSMS
Objective	• Project success can only be secured if qualified staff and sufficient material resources are available
Activities	• Depending on the size and type of the organization appropriate staff resources shall be provided for the planned data protection organization (e.g. data protection officer, data protection coordinators for each operating department / division / company) • Clarify the necessity of external resources • Provision of necessary financial means (budget), to achieve the defined project goals • Upon completion of the project it shall be secured that appropriate resources for the continuous maintenance of the DSMS will also be available subsequent to the implementation project
References	• Art. 24 DSGVO • ISO/IEC 27001 chapter 5.2

1.4 Initially instruct key staff	in preparation ☐ done ☐
Description	Key staff must be offered trainings in the fields of data protection and data security. With a compact overview of the new challenges key staff may develop within the organization to become important multipliers for data protection and data security. At the same time, it may thereby be secured that key staff can independently assume work packages within the implementation project for the DSGVO, resp. cooperate in work packages.
Objective	• Key staff is capable of explaining the importance of data protection and data security issues for the proper organization • Key staff is capable of documenting a processing activity, resp. of obtaining the information necessary therefore
Activities	Possible training content: • Principles and protection targets • What are personal data? • What are data subject to particular protection (special categories of personal data)? • Tasks and duties of key staff • Rights of persons concerned (information inquiries etc.) • Confidentiality obligations/data secrecy • Organization-internal consultation paths (data protection in internal projects, introduction of new software etc.)
References	• Art. 4, 5 -11 DSGVO • §§ 4 and 6 DSG

1.5 Check whether data protection officer (DSB) is required	in preparation ☐ done ☐
Description	Under certain circumstances the appointment of a DSB is mandatory. An organization shall therefore find out whether this rule applies in its own case and whether a DSB shall be appointed. Corporate groups and affiliated enterprises as well as official bodies should furthermore check whether one DSB is sufficient for the entire group or whether several DSBs shall be appointed.
Objective	• Determination whether one or more DSBs shall be appointed at all
Activities	Should one of the following criteria apply, it will be necessary to appoint a DSB: • Processing of data by an authority or official body with the exception of courts • Processing of personal data constitutes a core activity of the organization and/or requires an extensive regular and systematic monitoring of the persons concerned • Processing of special categories of personal data (e.g. health, ethnic origin etc.) or personal data on criminal convictions and offences constitutes a core activity of the organization
References	• Art. 37 DSGVO • Consideration reason 97

Phase 2: Implementation

2.1 Identify processing activities	in preparation ☐ done ☐
Description	In a first step all processing activities shall be identified and pivotal questions (responsible person, data types, data origin, data transfer etc.) shall be answered. Subsequently information may be consolidated, data flow analyses may be established and the results may be transferred to the procedure index.
Objective	• Identify processing activities • Document processing activities

Activities	1. Identify processing activities
	  ○ Applications
	  ○ IT-systems
	  ○ Document storage (e.g. in excel files etc.)
	  ○ Physical file
	  ○ *Tip:* Knowingly define the term "processing activity" broadly
	2. Creation of a template for recognition of current state
	  ○ Shall contain pivotal questions
	  ○ *Tip:* Excel-file, questionnaires or tool-support
	3. Pivotal questions as per processing activity:
	  ○ In which legal entities / sites / departments is the processing activity being performed?
	  ○ Who is responsible for the respective processing activity?
	  ○ Which personal data of which persons are being processed?
	  ○ What purpose are the data being processed for?
	  ○ What is the legal basis (e.g. contract compliance, acceptance declaration etc.)?
	  ○ Where do the data come from (origin)?
	  ○ Where do the data go to / whom are the data sent to?
	  ○ For how long are the data required / saved?
	  ○ *tip:* "Cleaning" - operation:
	  ▪ Which processing activities are no longer required?
	  ▪ Which data may be deleted?
	4. Persons involved:
	  ○ Contact person for data protection issues at the individual sites / operating department
	  ○ DSB (data protection officer), IT-manager, CISO, Legal department etc.
	  ○ Optional: External consultants (data protection experts, IT- / information security experts)
	5. Feedback of the compiled information to the project team
	6. Consolidation of all information received by the project core team
	  ○ Clarification of possible questions / elimination of ambiguities
	7. Establishment of data flow analysis as per processing activity by the project team
	  ○ Subsequently: Transfer of the information in the procedure index

References	• Art. 2, 3 and 30 DSGVO

2.2 Establish procedure index	in preparation ☐ done ☐
Description	The procedure index is an index of all processing activities. The person in charge as well as - to a smaller extent - the data processing company is obliged to maintain a procedure index. Maintenance of the procedure index shall be in writing, when an electronic format may be used. The procedure index shall be made available upon request of the regulatory authority. The procedure index enables the regulatory authority to control the processing activities performed.
Objective	• Registration of all processing activities with personal data within an organization, authority or official body, in case there is an obligation to maintain the procedure index

Activities	• Collect details of the processing activities in the role of the responsible person:
	  ○ Name and contact details of the responsible person resp. of the DSB
	  ○ Purpose of the processing activity
	  ○ Categories of persons involved (e.g. employee, customer, suppliers etc.) and categories of personal data (e.g. invoice details, address details etc.)
	  ○ Categories of recipients whom the personal data have been disclosed to or will be disclosed to (e.g. social insurance institution, tax authority, tax adviser etc.)
	  ○ If applicable, transfers of personal data to recipients in a third-party state (e.g. USA) or to an international organization, inclusive of statements of the concerned third-party state or of

	the concerned international organization (including the documentation of appropriate guarantees) ○ If possible: Scheduled deadlines for the deletion of various data categories ○ If possible: General description of TOMs (references to internal security guidelines from an ISMS are well appropriate here) ○ Reasonable: Statement of the legal basis (e.g. acceptance declaration) for the purpose of the processing activity • Collect details of the processing activities in the role of the data processing company: ○ Name and contact details of the data processing company, resp. of the DSB ○ Categories of processing which are being performed on behalf of each person in charge ▪ If applicable, transfers of personal data to recipients in a third-party state (e.g. USA) or to an international organization, inclusive of statements of the concerned third-party state or of the concerned international organization (including the documentation of appropriate guarantees) ▪ If possible: General description of TOMs (references to internal security guidelines from an ISMS are well appropriate here) • Recommendation: For practicability and clarity reasons also further-going information should be considered with the creation of a procedure index (e.g. data protection-consequences assessment, rights of the concerned person, information security etc.)
References	• Art. 12-21, 30 and 35 DSGVO • § 4 para 2 DSG • Consideration reasons 13, 75, 76 and 82

2.3 Check and if applicable perform data protection-consequences assessment	**in preparation ☐ done ☐**
Description	If from the point of view of the person concerned there is a presumable high risk, a data protection-consequences assessment shall be performed. With regard to certain processing activities which will anyhow require a data protection-consequences assessment, the regulatory authority will maintain a respective list. Besides there may also exist a list including exceptions.
Objective	• Analyse the consequences and risks of processing activities for the rights of concerned persons
Activities	• Phase 1: Pre-examination phase ○ Examination of the proper procedure index vis-à-vis the lists of the regulatory authority, whether a data protection-consequences assessment is mandatory (“Blacklist”) or not (“Whitelist”) ○ Examination whether at all the prerequisites are given for the performance of a mandatory data protection-consequences assessment (non-comprehensive catalogue of Art. 35 para 3) ▪ Will new technology be applied with the intended processing activity or will, due to the type, extent, circumstances and the purposes of the processing activity, the risk for the rights and liberties of concerned individuals be high? ▪ Will a systematic and comprehensive assessment of personal aspects of individuals be performed (profiling), which subsequently shall be used as the basis for decisions which might unfold legal consequences for the individuals (e.g. questions regarding the allocation of credits)? ▪ Are specific categories of personal data or data on criminal convictions and offences being processed in an extensive manner? ▪ Does systematic extensive monitoring of publicly accessible areas take place with the processing activity (e.g. video monitoring)? ○ Examination whether other criteria for the performance of a mandatory data protection-consequences assessment are given (e.g. criteria catalogue of the Art. 29 Group WP 248) • Phase 2: Assessment phase ○ Risk identification ○ Perform risk assessment as per each processing activity ▪ Probability of occurrence ▪ Effect / Damage ○ Risk treatment
References	• Art. 22 and 35 DSGVO • Consideration reasons 76, 84 and 89-93 • Best-Practice: ISO 31000, ISO 29134, BSI IT-Basic Protection • Working Paper 248 of Art. 29 group (http://ec.europa.eu/newsroom/document.cfm?doc_id=44137)

2.4 Secure compliance with the data protection-principles	in preparation ☐ done ☐
Description	Compliance with the data protection-principles shall be guaranteed, e.g. by asking control questions.
Objective	• Securing and documentation of compliance with the data protection-principles

Activities	• Lawfulness, processing in good faith, transparency
	  ○ Examination of the legal basis (e.g. contract with customers, acceptance declaration, compliance with laws)
	  ○ Control question: Has it been examined whether these personal data may be processed?
	  ○ Control question transparency: Is it possible to explain to the person concerned in a clear and comprehensible manner which personal data are being processed and how they are processed?
	• Data minimization and appropriation
	  ○ Verify that only for a certain purpose actually necessary personal data are being processed (e.g. turnstile instead of video monitoring for analysis of stream of visitors)
	  ○ *Control question appropriation* What are these personal data being used for?
	  ○ *Control question data minimization:* Are the entire personal data actually needed or can the same purpose be achieved with less resp. without personal data?
	• Store limit
	  ○ Examination of the existing statutory, resp. contractual retention obligations (e.g. configure systems in such a way that data which are no longer required are deleted automatically)
	  ○ *Control question:* For how long are these data required?
	• Correctness, integrity, confidentiality and availability
	  ○ Protection of data from loss, resp. destruction (e.g. backup), modification (e.g. checksums) and unauthorized access, resp. disclosure (e.g. authorization concept)
	  ○ Ensure that required data are available (e.g. by redundant systems in two server rooms)
	  ○ *Control question:* How has it been ensured that these personal data are materially correct, available and sufficiently protected?
	• Accountability
	  ○ Documentation of compliance with the data protection principles
	  ○ *Control question:* How is compliance with the data protection principles being documented?

References	• Art. 5 DSGVO • Consideration reason 39

2.5. Implement data securing measures (TOMs)	in preparation ☐ done ☐
Description	The responsible person shall take appropriate technical and organizational measures (TOMs), depending on the • state of the art • implementation costs • extent, circumstances and purposes of the processing as well as • the different probabilities of occurrence and the severity of the risk for the rights and liberties of individuals State of the art is usually represented by (inter)nationally acknowledged standards (e.g. ISO/IEC 27001:2013, BSI IT-Basic Protection etc.). These specifications shall be adapted to the conditions of the proper organization.
Objective	• Securing of appropriate TOMs • Compliance with the state of the art

Activities	Which TOMs have to be implemented? (acc. to Controls of the ISO/IEC 27002)
	• Pivotal information security specifications (Annex 5)
	  ○ Create IT-security-, resp. user guideline (e.g. security guideline, data protection policy)
	• Organization of information security (Annex 6)
	  ○ Define roles and responsibilities (e.g. CISO)
	• Staff security (Annex 7)
	  ○ Create processes for entry, team change and leaving (e.g. check lists for staff discharge)
	• Administration of values (Annex 8)
	  ○ Define competences and regulations for the return of values (e.g. devices, software, authorizations, keys)
	  ○ Classification of information (e.g. public vs. internal)

	• Access control (Annex 9)
	  ○ Define regulations for admission (e.g. key) and access (e.g. user administration, access to systems)
	  ○ Create password specifications (e.g. minimum length, complexity)
	• Cryptography (Annex 10)
	  ○ Create regulations for the handling of encoding (e.g. E-Mail encryption)
	• Physical and environment-related security (Annex 11)
	  ○ Define safety zones (e.g. fence or access control for data processing centre)
	• Operational safety (Annex 12)
	  ○ Manage and document operating procedures (e.g. Change management)
	  ○ Take measures for protection from harmful software (e.g. virus protection)
	  ○ Protect data from loss (e.g. backup)
	  ○ Introduce logging- and monitoring mechanisms (e.g. Logging)
	  ○ Define regulations for the handling of weak spots (e.g. input of security patches)
	  ○ Define measures for the installation of software (e.g. regulation of administrator rights)
	• Communication security (Annex 13)
	  ○ Take network security measures (e.g. Firewall, network segmentation, 802.1X)
	  ○ Ensure safe data transfer (e.g. encryption of transferred data)
	• Acquisition, development and maintenance of systems (Annex 14)
	  ○ Separation of development-, test- and production systems
	  ○ Create specifications for safe development (e.g. use of certain libraries)
	• Supplier relations (Annex 15)
	  ○ Create security specifications for suppliers and verify compliance (e.g. remote maintenance, on-site services)
	• Handling of information security incidents (Annex 16)
	  ○ Establish process for the handling of security incidents (e.g. define CERT)
	• Information security aspects with Business Continuity Management (Annex 17)
	  ○ Define regulations to ensure information security also in case of emergency (e.g. Integration CISO in case of emergency)
	• Compliance (Annex 18)
	  ○ Define regulations for compliance with statutory and contractual requirements
	
	Verification of compliance with the state of the art
	• Whether the security measure taken complies with the state of the art, may for example be verified vis-à-vis the requirements of a measure catalogue of the BSI IT Basic Protection
	  ○ Example: The measure catalogue M 2.11 “Regulation of password use” contains specifications regarding length, quality, complexity etc. of a password
	  ○ Such specifications are continuously kept up-to-date and represent to the greatest possible extent the state of the art

References	• Art. 32 DSGVO • Consideration reason 83 • ISO/IEC 27001:2013 and Controls of the ISO/IEC 27002:2013 • BSI IT-Basic Protection

2.6 Preserve the rights of concerned persons	in preparation ☐ done ☐
Description	Beside the extended duties of the responsible person according to Art. 12, 13 and 14 DSGVO (transparency and information), the responsible person has to observe extensive rights of the persons concerned and to ensure their timely fulfilment upon request.
Objective	• Ensuring of compliance with duties for the timely fulfilment of the rights of the persons concerned by introduction of organizational, technical and legal measures and processes

Activities	• Right to information (Art. 15 DSGVO)
	  ○ Examination of provision of remote access, resp. a copy of the concerned personal data (purposes, processed data, recipient, storage time, rights of persons concerned, data origin, automated decision making, transfer to third party countries etc.)
	• Right to correction (Art. 16 DSGVO)
	  ○ Correction of wrong data
	• Right to deletion resp. right to be forgotten (Art. 17 DSGVO)
	  ○ Examination and documentation of possible exceptions
	• Right to restriction of processing (Art. 18 DSGVO)
	  ○ Examination and implementation of marking / barring until decision on further processing activity
	• Right to transferability (Art. 20 DSGVO)
	  ○ Examination of applicability to existing data as well as examination of technical feasibility and implementation into the systems
	• Right to objection (Art. 21 DSGVO)
	• Determination and documentation of processes, in particular of responsibility
	  ○ Ensuring compliance of duties with the data processing company, if existing

References	• Art. 15 through 21 DSGVO • Consideration reasons 58 through 73

2.7. Introduce acceptance process	in preparation ☐ done ☐
Description	Unless the processing serves compliance with a contract or a legal duty, the lawfulness of the processing of personal data may be particularly ensured by the acceptance of an individual. Specifications of the DSGVO shall be observed in detail.
Objective	• Acceptance shall be made by unsolicited, unambiguous action manifesting that the person concerned agrees to the processing of the personal data relating to her-/himself • The responsible person has to be able to prove that the person concerned has expressed his/her acceptance with the processing activity • The person concerned shall be made aware who the responsible person is, what purpose his/her personal data are being processed for and that the acceptance may also be refused or withdrawn
Activities	• Obtain explicit, verifiable acceptance of the processing of personal data, e.g. enable ticking of a box when visiting a website (silence, already ticked boxes or inactivity do not constitute acceptance) • Creation of an acceptance declaration in comprehensible form and clear language (“no hiding in General Terms of Business”) • In case of an age under 16 (resp. 13, 14, 15 or 16, depending on national law; in Austria under the age of 14) the acceptance shall be obtained from the legal representative (e.g. parents) for an offer of services by the information company ○ Securing that in case of revocation of acceptance the data are no longer processed
References	• Art. 4 sub-para 11, 7 and 8 DSGVO • § 4 para 4 DSG • Consideration reasons 32, 38, 42 and 43

2.8 Introduce information duties	in preparation ☐ done ☐
Description	To ensure a fair and transparent processing of personal data, the responsible person shall make available to the persons concerned all information describing the type, purpose and extent of the processing activity. It is distinguished between data obtained directly from the person concerned or data reaching the responsible on a different way. The information duty does not have to be observed if the person concerned already disposes of all information related to the processing of his/her data.
Objective	• Establishment of precise, easily accessible, easily understandable information on the performed processing activity of personal data for persons concerned
Activities	If the data are obtained directly from the person concerned, the following information shall be made available at the time of ascertainment: • Name and contact details of the responsible person as well as his representative and of the DSB if applicable • The purposes which the personal data are processed for • The legal basis which the processing activity relies on • Insofar as the processing activity is based on the interest of the person in charge, the display of that interest • Recipient data if applicable • If applicable, the information on the transfer of the data to a third-party country and demonstration of the legal basis therefore • Time of storage of the data resp. the criteria for the determination of the duration • An indication of the rights of concerned persons to information, correction, deletion, revocation and data transfer • A reference to the right of complaint with a supervisory body • In case of automated decision making a description of the logic as well as of the consequences and the intended effect for the person concerned • If applicable, a description of all other purposes which the personal data shall be processed for beside the original purpose Insofar as the data have not been obtained directly from the person concerned, the abovementioned information and additionally the following information shall be made available within an appropriate period, after one month at the latest: • The categories of personal data which are processed • The source where the personal data come from (origin of data) Examples on how to comply with the information duty: • Making available of information on the Intranet • Provision of an information sheet within the scope of registrations (e.g. web shops) • Revision of data protection policy • Revision of company agreements
References	• Art. 12 through 14 DSGVO • Consideration reasons 58 through -62

2.9 Ensure framework conditions of data processing companies	in preparation ☐ done ☐
Description	A data processing company is a company processing personal data on behalf of a responsible person (e.g. cloud service provider, hosting-provider, software-provider, outsourced payroll accounting, service provider within a group of companies etc.) With the choice and commissioning of a data processing company certain framework conditions shall be ensured and agreed in writing.
Objective	• Choice of a data processing company providing sufficient guarantees that TOMs are being performed in such a way that the processing activity is made in accordance with the DSGVO • Written agreement of all legal duties arising for a responsible person by the cooperation with a data processing company (by way of binding clauses)

Activities	• Identification of all data processing companies and their sub-contractors
	• Examination of existing contracts with regard to minimum content of the DSGVO and updating of the same
	  ○ In case of conclusion of agreements before May 25, 2018, include the new duties already (to avoid renegotiations as of May 25, 2018)
	• Securing compliance with the duties of data processing companies (e.g. Consideration of the right to auditing)
	  ○ Careful choice of data processing company
	  ○ Regular examination whether the legal duties are being observed

References	• Art. 4 sub-para 8, 28 and 29 DSGVO • Consideration reasons 80 and 81

2.10 Ensure data protection by design / data protection by default	in preparation ☐ done ☐
Description	Data protection by design and data protection by default are two specifications for implementing data protection principles (e.g. Data minimization) - regarding technical (e.g. software) as well as organizational aspects (e.g. organization processes). Data protection by design means to detect and verify data protection risks already with the development of new technologies and to integrate data protection from the outset into the overall concept. Data protection by default means that products or services are by default configured in a data protection friendly way. In terms of accountability duty, the considerations and decisions shall be documented.
Objective	• Implementation of appropriate TOMs ensuring that the requirements for data protection by design and data protection by default are complied with • Definition and implementation of a processing of personal data with the lowest risk for the persons concerned
Activities	To achieve a most low-risk processing of personal data, the following protection measures shall be implemented (if applicable): • Minimize the quantity of personal data • Pseudonymizing and encryption of personal data as early as possible • Establish transparency regarding the functions and the processing of personal data • Delete or anonymize personal data as early as possible • Minimize access possibilities to personal data • Pre-set existing configuration possibilities in the most data protection friendly values • Documentation of the risk assessment for the persons concerned • Documentation of the set TOMs Examples: • Data Protection by Design: Features for pixelating personal data at the push of a button (e.g. for remote maintenance access, exports etc.) • Data protection by default: Data protection friendly basic settings in social networks
References	• Art. 25 DSGVO • Consideration reason 78

2.11 Introduce data breach process	in preparation ☐ done ☐
Description	A process shall be introduced on how the timely notification of data protection violations as well as the taking of appropriate countermeasures may be carried out.
Objective	• Data protection-conform course of process for the handling of data breaches defined • Ensure complete and timely information to supervisory body and if applicable to persons concerned

Activities	Preparation data breach (all activities shall be defined in a first step to be able to work them off as quickly as possible in case of occurrence):
	• Identify process-related dependencies and available resources
	• Determine roles and responsibilities
	  ○ Who does what and when?
	  ○ Who has to take decisions and which?
	  ○ Which roles is the CERT composed of?
	• Recognise and record incident (pre-emtively / reactively)
	  ○ Integration of possible third parties (such as in particular data processing companies)
	• Perform first assessment
	• Take immediate measures
	• Information to the responsible person (e.g. top management)
	• Secure public relations (e.g. institution of “emergency”-hotline)
	• Information of the persons concerned:
	  ○ Formulation in clear and simple language
	  ○ Description of the type of violation of the protection of personal data
	  ○ Approximate number of personal data files concerned
	  ○ Names and contact details of the DSB or any other contact person for further information
	  ○ Description of probable consequences of violation of protection of personal data
	  ○ Description of the measures taken or proposed by the responsible person for the removal of the violation of the protection of personal data
	  ○ If applicable, description of measures for the attenuation of its possible detrimental consequences
	• Information to the supervisory body within 72 hours
	  ○ Minimum information to the supervisory body:
	  ▪ Description of the type of violation of the protection of personal data, as far as possible by statement of
	  • the categories of the persons concerned,
	  • the approximate number of persons concerned,
	  • the concerned categories of personal data files and
	  • the approximate number of personal data files concerned
	  ▪ name and contact details of the DSB or any other contact person for further information
	  ▪ Description of probable consequences of violation of protection of personal data
	  ▪ Description of the measures taken or proposed by the responsible person for the removal of the violation of the protection of personal data
	  ▪ Documentation of all violations of the protection of personal data including related facts
	• Taking of (subsequent-) measures
	  ○ Lessons learned by the incident (KVP)
	• Note: A data processing company shall undertake by contract that a data breach will be notified immediately, resp. that a cooperation duty exists with the remedying of the data breach

References	• Art. 28 para 3 sub-para f, 33 and 34 DSGVO • Consideration reasons 85 through -88

2.12 Tasks of the data protection officer (DSB)	in preparation ☐ done ☐
Description	The DSB monitors the compliance with the DSGVO as well as with other applicable data protection provisions. The DSB is the first point of contact internally and externally in questions of data protection and advises amongst others with the procedure index and the data protection-consequences assessment.
Objective	• Monitoring of compliance with the DSGVO, the DSG (Data Protection Act) and other data protection provisions • Consulting and controlling activities
Activities	• Contact person for the supervisory body and for concerned persons • Consulting in data protection questions for employees • Consulting of top management, employees and concerned persons • Training of employees • Monitoring of the implementation of a DSMS • Monitoring of and consulting with the data protection-consequences assessment • Monitoring of and consulting with the procedure index • Direct reporting to the top management • Performance of an internal data protection audit
References	• Art. 39 DSGVO • Consideration reason 97 • Working Paper 243 rev. 01 of Art. 29 Group (http://ec.europa.eu/newsroom/document.cfm?doc_id=44100)

2.13 Establish data protection policy	in preparation ☐ done ☐
Description	Creation of a high-level document with binding and pivotal data protection specifications from an organizational point of view, which shall be put into force by the top management.
Objective	• Recording and proof of the regulations and specifications established within the scope of the DSGVO-compliance • Alliance of guidelines with procedure index and data protection-consequences assessment
Activities	• Investigation and updating of already existing specifications (also of used practice) • Integration of required persons / committees with necessary know-how • Determination of form, applicability and announcement / availability of the data protection policy • Planning and organisation of establishment of the data protection policy • If applicable, alignment with available samples, rules of behaviour resp. binding internal data protection provisions
References	• Art 5, 24, 32, 40, 42 and 47 DSGVO • Consideration reasons 39, 74 -77, 83, 98 - 100 and 110

2.14 Train employees	in preparation ☐ done ☐
Description	Training of all employees who are dealing with personal data regarding • the DSGVO and other applicable data protection provisions, • important provisions within the organization (e.g. data protection policy) as well as • the consequences in case of non-compliance
Objective	• Employees shall be aware of the fact that personal data are subject to protection and that also information security aspects shall be observed • Employees shall understand what exactly personal data are, where they have to do with them and what they need to / may / may not do (e.g. compliance with data secrecy) • Employees shall understand the rights of persons concerned in order for them to realize the consequence on their daily work as well as their responsibility • Permanent procurement of knowledge by continuous awareness trainings

Activities	• Employees shall receive a basic training for data protection, but equally for information security where the interleaving of the themes is displayed also in the operational practice (e.g. which measures with regard to data protection and information security exist in this organization etc.)
	• Examples for training types:
	  ○ Presence-training, eLearning, Workshop etc.
	• Documentation of the training (e.g. list of signatures)
	  ○ Securing of regular trainings

References	• Art. 39 and 47 DSGVO • § 6 DSG • Consideration reasons 97 and 110

2.15 Data transfer (EU / international)	in preparation ☐ done ☐
Description	Personal data may only be transmitted to third party states outside the EU without appropriate protection level, if it is ensured by respective processes and mechanisms that the requirements of the DSGVO are observed.
Objective	• Securing of compliance with the lawfulness when transmitting personal data to third party countries • Introduction of processes with planned data transfers with international reference

Activities	• Examination of existing data flows to third party states outside the EU
	• Examination of authorization facts according to the DSGVO, in particular
	  ○ Adequacy resolution (Art. 45)
	  ○ Examine adequate guarantees or adapt existing ones (Art. 46 and 47) (e.g. binding corporate rules, standard agreement clauses of the supervisory bodies, rules of behaviour, mechanisms of certification)
	  ○ Verification of exceptions for certain cases (Art. 49), in particular: Acceptance of the person concerned, contract, important public interest, legal claims, vital interests, transmission from register
	  ○ Implementation of processes for securing that with future processing activities the transfer of personal data to third party countries will be respectively considered and regulated

References	• Art. 44 through 49 DSGVO • Consideration reasons 101 through 115

Phase 3: Current activities

3.1 Update procedure index	in preparation ☐ done ☐
Description	After the first establishment based on an extensive data collection the procedure index shall be updated continuously.
Objective	• Securing that the procedure index is at all times up to date • Securing that new processing activities are integrated in the procedure index

Activities	• Determination of a timetable for the regular examination of the procedure index
	• Organizational securing that the persons responsible for the procedure index are informed on modifications in due time.
	  ○ Further / different data types
	  ○ Further / different persons concerned
	  ○ Change of purpose, resp. extension
	  ○ Entry of new recipients
	  ○ Modified storage- resp. deletion periods
	  ○ Documentation of the adaptation of the TOMs or appropriate guarantees
	  ○ Adaptation of the underlying documents (e.g. acceptance declaration, contracts, company agreements etc.)
	• Examination of the currentness of the data protection-consequences assessment (if applicable updating of an existing data protection-consequences assessment or performance of a data protection-consequences assessment)
	• Include new processing activities in the procedure index, resp. delete no longer existing processing activities from the procedure index
	  ○ Regular presentation of the procedure index to the top management

References	• Art. 30 and 35 DSGVO • § 4 para 2 DSG • Consideration reasons 82 and 84 -89

3.2 Perform audits	in preparation ☐ done ☐
Description	Similar to other management systems, the effectiveness and the efficiency of a DSMS shall be examined regularly. This includes the performance of regular internal resp. external audits for the monitoring as well as the deduction of respective measures for the continuous improvement of the DSMS. For example, existing management systems (e.g. ISMS according to ISO/IEC 27001) may also be aligned with the DSMS.
Objective	• Maintenance and improvement of the effectiveness of the DSMS

Activities	• Planning of the regular audits
	  ○ Determination of the respective scope
	  ○ Agreement on and planning of the interviews
	  ○ Request for the documents to be examined
	• Exemplary performance of the data protection audit
	  ○ Review of the procedure index, of the data protection policy, of the process results and of other relevant documents
	  ○ Performance of the interviews
	  ○ If applicable, performance of specific audits of systems and the respective data flow
	• Establishing the report
	  ○ Description of identified deviations within the DSMS
	  ○ Deduction of measures for the handling of the identified deviations
	• Report to the top management
	  ○ Reporting of the status and of the improvement measures
	  ○ Building, resp. renewal of awareness

References	• Art. 24 DSGVO • ISO/IEC 27001 chapter 9.2

3.3 Maintain contact with authorities and concerned persons	in preparation ☐ done ☐
Description	Contact with authorities and concerned persons should be established and maintained preventively, to dispose of respective communication channels in case of need.
Objective	• Maintenance of the contacts as well as cooperation with the supervisory body and concerned persons • Meet expectations of authorities as well as of customers and employees upon transparent and secure handling of data

Activities	• Establishment of an overview of interested parties (e.g. stakeholders etc.)
	  ○ Supervisory body
	  ○ Other authorities (e.g. NIS, RTR, BMI, FMA, various CERTs)
	  ○ Concerned groups of people
	  ○ Public (e.g. Media etc.)

References	• Art. 31 and 57 DSGVO

3.4 Secure KVP (continuous improvement process) of the data protection-management system (DSMS)	in preparation ☐ done ☐
Description	Continuous improvement of suitability, appropriateness and effectiveness of the DSMS as well as co-integration of legal modifications (e.g. decisions, regulations etc.).
Objective	• Securing of continuous legal conformity by regular adaptations of the DSMS

Activities	• Recognition and removal of non-conformities
	• Documentation of non-conformities as well as of correction measures
	• Continuous evaluation resp. improvement of ...
	  ○ TOMs / state of the art / threat situation
	  ○ Awareness of employees
	  ○ Data protection policy
	  ○ Data protection relevant processes (e.g. information, acceptance etc.)
	  ○ Contracts (e.g. with data processing companies, SLAs, standard data protection clauses)
	  ○ Internal resp. external audits

References	• Art. 24 DSGVO • ISO/IEC 27001:2013 chap. 10