



The Processing Records

Records of Processing Activities
according to Art. 30 General Data Protection
Regulation (GDPR)

Publisher

Bitkom e. V.
Federal Association for Information Technology, Telecommunications and New Media,
Albrechtstraße 10 | 10117 Berlin

Contact

Susanne Dehmel | Member of the Executive Board for Law and Security
+4930 27576-223 | s.dehmel@bitkom.org

Authors

- Wolfgang Braun, Group Data Protection Officer Giesecke & Devrient GmbH
- Susanne Dehmel, Member of Executive Board Bitkom e.V.
- Heiko Gossen, Managing Partner migosens GmbH Bernd H. Harder, Harder Attorneys at Law
- Dr. Hartmut Hässig, Data Protection Officer EMC Deutschland GmbH
- Lars Kripko, Consultant for Data Protection and External Data Protection Officer T-Systems Multimedia Solutions GmbH
- Ilona Lindemann, Data Protection Officer gkv informatik GbR
- Christian Wagner, Data Protection Officer Nokia Solutions and Networks GmbH & Co. KG
- Stephan Weinert, Data Protection Officer Computacenter AG & Co oHG

Graphics & Layout

Coco Collmann | www.coco-collmann.de

Cover

© weerapat1003 – Fotolia.com

Copyright

Bitkom 2017

This publication constitutes general, non-binding information. The content represents the views of Bitkom at the time of publication. While great care is taken in preparing this information, no guarantee can be provided as to its accuracy, completeness, and/or topicality, in particular, this publication does not take into consideration the specific circumstances of individual cases. The reader is therefore personally responsible for its use. Any liability is excluded. All rights, including all rights to partial publication, reserved.

The Processing Records

Records of Processing Activities
according to Art. 30 of the General Data Protection
Regulation (GDPR)

Table of Contents

Preface to Version 4.0	4
1 Introduction	5
2 Records of Processing Activities	6
2.1 Definitions	6
2.2 Purpose and Objective of the Processing Records	6
2.3 Obligation to maintain Processing Records	6
2.4 Responsibilities	8
2.4.2 The Data Protection Officer	11
2.4.3 Joint Controllershship	10
2.4.4 Responsibilities with regard to processing on behalf of the controller	10
2.4.5 Controllers or Processors not established in the Union and the Representatives	11
2.5 Contents and structure of the processing records	11
2.5.1 Mandatory disclosures in the record of processing activities of the controller	14
2.5.2 Mandatory disclosures in the record of processing activities of the processor	15
2.5.3 Internal additional information in the record of processing activities of the controller	16
2.5.4 Internal additional information in the record of processing activities of the processor	18
2.6 Definition of a processing	19
2.7 Form of the processing records	20
3 Creating the processing records	21
3.1 Sensitization phase	22
3.2 Information phase	22
3.3 Query phase	23
3.4 Advisory phase	23
3.5 Consolidation phase	24
3.6 Implementation phase	24
3.7 Data Protection Impact Assessment and Admissibility Check	25
3.8 Maintenance phase	28
4 Software for managing the processing records	27
5 Appendix	28
5.1 Examples of Processing Records	28
5.1.1 Example of a processing record of the controller established in the EU	28
5.1.2 Example of a processing record of representative of a controller established outside of the EU	30
5.2 Example of a processing record of a processor	31

5.3	Forms for compiling the processing records _____	32
5.3.1	Form: recording a processing activity _____	32
5.3.2	Form: Notification of a negative report _____	37
5.3.3	Form for internal confirmation notes of the data protection officer _____	38
5.3.4	Explanation of the forms _____	39
5.4	Providers of software for compiling processing records _____	42

Preface to Version 4.0

The last guide for keeping a processing directory (3.0) in accordance with the requirements of the Federal Data Protection Act (BDSG) has been published by Bitkom in spring 2016. Due to the General Data Protection Regulation's (GDPR) entry into force in May 2016 and the applicability of the new rules from May 2018 onwards, the regulations of the BDSG for keeping a processing directory will be replaced by EU-wide applicable standards. The term processing directory will be replaced by the term record of processing activities. The existing general reporting requirement governed by § 4d para 1 BDSG is no longer applicable, whereas a general obligation of the controller to provide evidence and to document the legality of the processing is anchored in Article 24 para 1 GDPR. The Regulation also contains an explicit duty of the controller and (new) processors to keep a record of processing activities (Article 30 GDPR). The latter obligation does not apply to enterprises or organizations with less than 250 employees, who process only to a limited extent and non-sensitive data (Article 30 para 5 GDPR).

Thus, the documentation of data processing in companies remains an important task and is the basis for the legitimate and legally certain processing of personal data. This is all the more true due to the tremendously increased fines for data protection violations in the GDPR. The documentation, however, not only provides evidence to the supervisory authorities, but also helps to implement and monitor all other duties of the controller towards the data subject with regard to the data processing (e.g. information and disclosure rights, deletion). For the data protection officer, the documentation is an important tool in completing his tasks. Therefore, considerations with regard to the record of processing activities are necessary either way – even if the company is not obliged under the new GDPR regime to keep such a record.

Special thanks go to the authors of this guide, their expertise and commitment which made the development of this guide possible:

- Wolfgang Braun, Group Data Protection Officer Giesecke & Devrient GmbH
- Susanne Dehmel, Member of Executive Board Bitkom e.V.
- Heiko Gossen, Managing Partner migosens GmbH Bernd H. Harder, Harder Attorneys at Law
- Dr. Hartmut Hässig, Data Protection Officer EMC Deutschland GmbH
- Lars Kripko, Consultant for Data Protection and External Data Protection Officer T-Systems Multimedia Solutions GmbH
- Ilona Lindemann, Data Protection Officer gkv informatik GbR
- Christian Wagner, Data Protection Officer Nokia Solutions and Networks GmbH & Co. KG
- Stephan Weinert, Data Protection Officer Computacenter AG & Co. oHG

Berlin, 28 April 2017

1 Introduction

Data protection plays an important role in modern data processing and is gaining economic importance. This can be seen not only in the increase in media attention with regard to sensitive legislative proposals and data protection violations, but also in the increased awareness with regard to the rights concerned. Key features of the European data protection legislation are, apart from the prohibition principle, the right to information and the transparency requirements concerning the data subjects.

Without meaningful and up-to-date documentation ensuring the rights concerned, as well as giving proof of the fulfillment of the obligations to the supervisory authorities is an intricate task and might well lead to an uncertain outcome.

Keeping records of processing activities is a form of documentation and a vital tool of data protection law for the implementation of the transparency obligations.

The following guideline explains the terms and principles of the records of processing activities and illustrates the process for creating such documentation. The authors of this guideline, data protection officers of companies, pay special attention to the practicability, regardless the company size.

2 Records of Processing Activities

2.1 Definitions

Article 30 of the GDPR obliges companies to maintain “records of processing activities”. The shorter term “processing records” is also used which is based on the earlier term “processing directory”.

The current legal status under the BDSG (until 25.05.2018) already requires a register of proceedings, (processing directory), which, in part, had to be open to view for anyone upon request.

Often, in practice, different terms were used for this legally required documentation.

The predecessor to this guide used the term “public processing directory” (öffentliches Verzeichensverzeichnis) for the documentation intended for public information, in practice and in literature, the terms “public registry” (“Jedermannverzeichnis”) and “processing directory” (“Verzeichensverzeichnis”) were coined.

The GDPR does neither provide for an opportunity or right to access to the registry for the public nor for a duty to register the company’s procedures.

Therefore, the distinction between “public” and “internal”, is no longer necessary. However, the supervisory authority can request the processing records. As the processing records can be extended and some meaningful documentation added, without these additions being legally required, however, the term “extended processing records” will be used.

2.2 Purpose and Objective of the Processing Records

The processing records serve to ensure transparency with regard to processing personal data and to provide legal protection for the company. It can support the company's data protection officer, as well as the supervisory authority in carrying out their tasks. In accordance with Article 30 para 4 of the GDPR, the controller or the processor shall make the record available to the supervisory authority on request. The processing records also serve as verification, so the company can prove to the supervisory authority that the requirements of the GDPR were fulfilled by the controller. Part of the general duty of the controller is the cooperation with the supervisory authority, on request, in the performance of its tasks (Article 31 of the GDPR).

The processing records are therefore not only the basis for fulfilling the controller's or processor's managerial duties, but also support the data protection officers in fulfilling their tasks.

2.3 Obligation to Maintain Processing Records

The obligation to maintain processing records is stipulated in Article 30 of the GDPR. According to Recital 82 the record is used as proof for compliance and demonstration of accountability with the GDPR rules.

The scope of the obligation to documentation covers all processing activities of the controller.

In principle, every controller is subject to the obligation to maintain such a record of processing activities. While two or more controllers, who have joint control over the purposes and means of processing, are so called “joint controllers”, not every one of them is obligated to maintain the records himself. Rather, joint controllers can conclude an agreement on which of them has to fulfill which obligations of the GDPR, and can therefore also determine who maintains the records. The processor also has to maintain records on all categories of processing activities carried out by the processor on behalf of the controller.

If the controller or processor is not established in the Union and therefore has to designate a representative in the Union, this representative is also obliged to maintain processing records. The obligation to maintain the processing records shall not apply to an enterprise or an organization employing fewer than 250 persons. However, the obligation is only omitted if the processing the enterprise or organization carries out is not likely to result in a risk to the rights and freedoms of data subjects, the processing is occasional, and if the processing does not include special categories of data as referred to in Article 9 para 1 or personal data relating to criminal convictions and offences referred to in Article 10 of the GDPR.

The very complicated wording of this exception is, especially when considering today's digital world, likely to result in very few companies benefitting from the exception to the obligation to maintain processing records.

The controller or the processor, as well as, if necessary, their representative shall, on request, provide the supervisory authority with the processing records. An obligation for a registration, as provided in the BDSG and the Data Protection Directive, is not included in the GDPR. The obligation to provide the supervisory authority with the processing records substantiates the obligation to cooperate with the supervisory authority, as provided in Article 31 of the GDPR.

Maintaining processing records is an excellent basis for compiling, and keeping available, the necessary information for the accountability and documentation obligations.

The accountability requirements provided by the GDPR include:

- Lawfulness, fairness, transparency
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality

The processing records can be valuable for the data protection impact assessment as it can be used to estimate the probability of a risk occurring and the severity of this risk regarding the rights and freedoms of the data subject in terms of nature, scope and circumstances as well as the purposes of the processing. The processing records are used to assess the legality of the processing operations, especially with regard to consent. Documentation of technical and organizational measures (TOMs) taken is an integral part of the documentation and thus the primary source for the assessment of the adequacy of the measures.

These reasons speak for keeping such processing records, even if the company is not legally obliged to do so. The processing records are an invaluable collection of all information regarding the processing of personal data for the controller and the data protection officer.

2.4 Responsibilities

Regarding the question with whom the responsibilities lie, a differentiation must be made between the formal responsibility on the one hand and the practical execution within the company on the other hand. Additionally, when defining the processing activities, consideration must be spent on whether the processing at hand is a processing on behalf of the controller, joint processing, or a transfer to a third party¹, as the mandatory information requirements differ for each processing.

2.4.1 Management

The formal responsibility to prepare and properly manage the processing records lies with the company management of the controller, or respectively of the processor. According to Article 30(1) of the GDPR, the manager has the responsibility to maintain the processing records. At the same time, according to Article 38 of the GDPR, the controller has to 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 (para 1), and the controller and processor shall support the data protection officer in performing his tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge (para 2).

¹ Further explanation regarding the differentiations between these types of processing can be found in these guidelines in “accompanying notes on the model contract for processing”.

In practice, the data protection officer often takes over the management of the processing records, especially the preparation of the procedural notifications, however, is the responsibility of the department and not the data protection officer. The data protection officer shall work toward the creation of the records and provide assistance, but bear no responsibility for the content of the records. Responsibility for the individual procedures remains with the departments and ultimately with the management of the controller.

The term controller refers to the smallest legally independent entity. This is the natural or legal person, authority, entity or other body, which alone or with other controllers determines the purposes and means of processing of personal data. This definition is explicitly laid down in Article 4(7) of the GDPR. For companies, this means that the controller is not the organizational entity (division, department, unit, or branch) that actually stores or processes the data (e.g. the data center or the human resources department), but the legal person (e.g. the GmbH, Ltd., BV) to which the organizational entity belongs.

Every company with legal personality is therefore a controller. Hence, separate processing records must be maintained for each company within a group and all subsidiaries. This can, however, be different in cases of joint controllership ([↗see under 2.4.3.](#))

Note

In principle, every legally independent company is a controller as defined by Article 4 of the GDPR.

2.4.2 The Data Protection Officer

The GDPR provides for no explicit connection between the data protection officer and the processing records. Maintaining processing records is neither one of his own responsibilities nor is he required to issue specifications regarding the records. However, in practice, it has proven successful to also consider the requirements of the data protection officer when compiling and maintaining the processing records.

If the data protection officer carries out the task of maintaining the processing records, he himself can, with the support of all business units, manage compiling and updating the records and can ensure the quality standards of the results. With this, he also fulfills the important function of providing the departments with comprehensible explanations and practical examples to enable the preparation of their information notices regarding the processing of personal data and facilitate the completion of provided forms. In this way, he can have an important influence on data protection compliance within the company.

2.4.3 Joint Controllership

In Article 26 the GDPR provides for the possibility of two controllers being jointly responsible for one or more data processing operations. This requires that they jointly determine the purposes and means of processing and lay down their respective responsibilities in an agreement². It should also be specified who is responsible for maintaining the processing records. The controller responsible must maintain the processing records and shall also list, in accordance with Article 30 para 1 subpara a of the GDPR, the other joint controller.

2.4.4 Responsibilities with regard to processing on behalf of the controller

When a company transfers individual data processing tasks or even the entire data processing to a processor so the processor carries out the processing on behalf of the controller pursuant to Article 28 of the GDPR, e.g. by order of outsourcing, it is important to clarify who is responsible for which part of the documentation of the processing.

Different from the BDSG, the GDPR contains a separate provision, Article 30(2), for the obligation of the processor to maintain processing records. He is required to maintain a record of all categories of processing activities carried out on behalf of a controller. Article 30(2)(a)-(d) of the GDPR lists the contents of these records. Article 30(4) of the GDPR provides for an obligation for the processor to make the record available to the supervisory authority on request.

At the same time, however, the controller is obliged to comply with Article 30(1) of the GDPR and maintain processing records of all processing activities subject to their responsibility.

Regarding this, it is necessary to consider the processor's own responsibility to maintain processing records, e.g. when he himself is the controller (e.g. processing data of their own employees), as he is obliged to provide documentation regarding the information mentioned [in 5.1](#). Therefore, in practice, the processor will have to maintain two processing records: one for his own processing as controller and one for processing done on behalf of another controller (his customer).

The contents of the processing records maintained by the processor and the controller differ according to their respective sphere of responsibility. While the controller has to specify the purpose of the processing as well as the categories of data and the recipients, the processor has to indicate the categories of processing carried out on behalf of the controller ([s.2.5.1](#)). According to Article 31 of the GDPR both the processor as well as the controller shall cooperate, on request, with the supervisory authority in the performance of their tasks.

² Further explanations can be found in the explanatory notes on the "Template Agreement Annex – Processing of personal data on behalf of a controller in accordance with Article 28 (3) of the EU General Data Protection Regulation (GDPR)" and the checklist on joint controllership.

2.4.5 Controllers or Processors not established in the Union and the Representatives

Controllers or processors not established in the EU who process data to which the GDPR applies shall designate a representative in the Union pursuant to Article 27 para 1 of the GDPR if their processing is not only occasional and does not include special categories of data (Article 28 para 2 subpara a of the GDPR) and the requirements of Article 3 para 2 of the GDPR are met. These representatives shall be a point of contact for supervisory authorities and data subjects in all matters relating to the processing and to ensure compliance with the GDPR (Article 27 para 4 of the GDPR). According to Recital 80 of the GDPR, the representative shall act in the name of the controller or processor. The controller or processor should expressly appoint the representative to do so and should, in writing, appoint him to act in his stead with regard to the obligations under the Regulation.

Article 30 para 1 of the GDPR mentions the representative as follows: “Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.” The wording suggests that the legislator assumed that, if a representative was designated, the representative would maintain the processing records for the assigned processing tasks.³

This is plausible to the extent that the representative will most likely be the one from which the supervisory authority will request the processing records. This is, however, the only indication in the Regulation that the representative should be the one to maintain the processing records. Theoretically, the controller could maintain the records himself, as long as he ensures that the representative can access the records if necessary.

2.5 Contents and structure of the processing records

The person responsible⁴ for handling and maintaining the processing records for the controller has to decide on how to keep the processing records at the beginning of his activity. His approach should be based on structure and complexity of the company. The degree of detail should also comply with the requirements set out by the data protection officer. At the same time, the processing records must be developed in a way that satisfies the legal requirements of Article 5 para (2) of the GDPR (“Accountability”), as well as the provisions of Article 24 and 30 of the GDPR.

³ Plath, in: Plath (ed), BDSG/DS-GVO (2nd edn 2016), Article 27 para 6: Furthermore, according to Article 30(1) of the GDPR, the representative is obliged to maintain the processing records.

⁴ The following explanations assume that the controller will appoint the data protection officer to handle and maintain the processing records. If another person is appointed to do so, the explanations regarding the processes necessary can be adapted.

In order to avoid unnecessary duplications, it is possible to refer to already existing documents in the processing records, e.g. with the general safety concept or the overarching TOMs. It should be noted, however, that these documents must also be provided to the supervisory authority if requested.

processing records of the controller

Requirements	General Information	<p>Company</p> <ul style="list-style-type: none"> ▪ if necessary, representative ▪ contact details of the data protection officer 		
	Procedure 1	Procedure 2	Procedure n	
	<ul style="list-style-type: none"> a) if applicable, other joint controllers b) purpose c) groups concerned and categories of data d) recipient e) standard periods for erasure f) intended transfer to third countries 	<ul style="list-style-type: none"> a) if applicable, other joint controllers b) purpose c) groups concerned and categories of data d) recipient e) standard periods for erasure f) intended transfer to third countries 	<ul style="list-style-type: none"> a) if applicable, other joint controllers b) purpose c) groups concerned and categories of data d) recipient e) standard periods for erasure f) intended transfer to third countries 	
	technical and organizational measures	overlapping TOMs / security concept		
		additional, alternative TOMs 1	additional, alternative TOMs 2	additional, alternative TOMs n
Extension	Applications and persons with access authorization	Application A: function and authorization	Application B: function and authorization	Application C: function and authorization
	Internal additional information	Legality data minimization information requirement data portability results of the risk assessment/data protection impact assessment	Legality data minimization information requirement data portability results of the risk assessment/data protection impact assessment	Legality data minimization information requirement data portability results of the risk assessment/data protection impact assessment
	optional: internal detailing	<div style="display: flex; justify-content: space-around; padding: 5px;"> <div style="border: 1px solid #0070C0; padding: 2px;">sub-procedure 1.1</div> <div style="border: 1px solid #0070C0; padding: 2px;">sub-procedure 1.2</div> <div style="border: 1px solid #0070C0; padding: 2px;">sub-procedure 1.3</div> </div>	<div style="display: flex; justify-content: space-around; padding: 5px;"> <div style="border: 1px solid #0070C0; padding: 2px;">sub-procedure 2.1</div> <div style="border: 1px solid #0070C0; padding: 2px;">sub-procedure 2.2</div> <div style="border: 1px solid #0070C0; padding: 2px;">sub-procedure 2.3</div> </div>	<div style="display: flex; justify-content: space-around; padding: 5px;"> <div style="border: 1px solid #0070C0; padding: 2px;">sub-procedure n.1</div> <div style="border: 1px solid #0070C0; padding: 2px;">sub-procedure n.2</div> <div style="border: 1px solid #0070C0; padding: 2px;">sub-procedure n.3</div> </div>

fig 1: Processing Records

2.5.1 Mandatory disclosures in the record of processing activities of the controller

According to Art. 30 para 1 a) to g) GDPR the following details must be provided in the record of processing activities of the controller:

Art. 30 para. 1	Contents	Comments
a)	the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer	This information serves the purpose of a transparent and unambiguous identification of the controller (company or organization) and the responsible persons.
b)	the purposes of the processing	The legal basis of the data processing must be inferable from the purpose of the processing. In practice, the tasks and aims of each individual processing are stated, e.g. "Human Resource Management"
c)	a description of the categories of data subjects and of the categories of personal data	This refers to the groups of persons whose data are processed in the individual processing, e.g. "employees" or "customers". Examples for categories of personal data are master data (e.g. contact data), motion data and usage data, etc.
d)	the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations	It is generally recommended to name the natural or legal persons, authorities, institutions or other bodies that shall receive the data orderly, regardless of whether it is an active transmission or a direct access of the recipient to the processing. This can be internal or external bodies as well as service providers within the scope of processing on behalf of the controller.
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 para 1, the documentation of suitable safeguards	Data transfers pursuant to the second subparagraph of Article 49 para 1 are such transfers that are exceptionally permissible, although neither an adequacy decision as referred to in Article 45(3) has been issued, nor appropriate safeguards as referred to in Article 46 exist.
f)	where possible, the envisaged time limits for erasure of the different categories of data	The phrase "if possible" must not be understood as optional, but in the sense that an erasure rule shall be stated as specific as possible. Usually the erasure depends on the purpose of the data collection and the use of the data. In principle, erasure must be carried out without delay after the fulfillment of the purpose of the data collection. Exceptions may arise out of the existence of special legal requirements to retain data, such as tax law or other sector-specific legislation.

Art. 30 para. 1	Contents	Comments
g)	where possible, a general description of the technical and organizational security measures referred to in Article 32(1)	Here, referrals can be made to the general safety concept / overarching TOMs, so that only deviations for the respective processing must be listed separately. In the case of referring to a document of reference, the latter must also be submitted to the supervisory authority where applicable.

2.5.2 Mandatory disclosures in the record of processing activities of the processor

According to Art. 30 para 2 a) to d) GDPR the following details must be provided in the record of processing activities of the processor:

Art. 30 para. 2	Contents	Comments
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	This wording is to some extent unclear. However, it may well be understood in such a way that, in addition to the contact details of the processor himself, at least the contact details of the controller, or if these contact details are unknown to the processor (e.g. because he is only one of several employed processors), the contact details of his direct employer must be given.
b)	the categories of processing carried out on behalf of each controller	In most cases, the categories of processing may correspond to the generally offered / agreed upon services of the processor and can mostly be inferred from the agreement of the processing on behalf of the 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 para 1, the documentation of suitable safeguards	Data transfers pursuant to the second subparagraph of Article 49 para 1 are such transfers that are exceptionally permissible, although neither an adequacy decision as referred to in Article 45(3) has been issued, nor appropriate safeguards as referred to in Article 46 exist.
d)	where possible, a general description of the technical and organizational security measures referred to in Article 32 para 1	Here, referrals can be made to the general safety concept / overarching TOMs, so that only deviations therefrom for the respective processing must be listed separately. In the case of referring to a document of reference, the latter must also be submitted to the supervisory authority where applicable.

2.5.3 Internal Additional Information in the Record of Processing Activities of the Controller

It should be individually decided for each company whether it is reasonable to include additional information which are documented by the company. This can be appropriate for information that the company needs in order to prove the legality of the processing in case of doubt. An obligation of the company to being able to demonstrate such compliance is regulated in Article 5 para 2 and Article 24 of the GDPR. Thus, the record of processing activities provides an opportunity to implement a structured documentation that is required by the GDPR in different provisions and to comply with the obligation to provide proof in Article 5 para 2 GDPR (at least the parts that can be documented in each processing).

Article	Content	Comment
Art. 5 para 1 a Art. 6	Legality a) Legal basis b) Consideration of specific categories of personal data, where necessary special obligations for confidentiality of certain employees (secrecy of social data) c) Compatibility in case of change of purpose d) Compliance with the requirement for consent (e.g. documentation of the consent clause, including historicization and confirmation note) e) Consideration of objections (e.g. can they be taken into account, where necessary reference to the nature of the process) f) Automated individual decision-making	To comply with the accountability obligations in Art. 5, the controller should not only demonstrate compliance with the requirement of compulsory recording of the purpose of the processing, but also the legal basis together with any necessary considerations, consent clauses and confirmation notes, and whether the requirements for the possibility of objections and the automated individual decision-making have been considered.
Art. 5 para 1 c Art. 25	Data minimization Privacy by design Privacy by default	This can be documented, e.g. by means of a confirmation note of the data protection officer indicating whether these requirements have been sufficiently considered.
Art. 5 para 1 d Art. 5 para 1 e	Accuracy of the data Storage Limitation / deletion or restriction of processing	Documentation e.g. with reference to measures and processes and how they are ensure
Art. 12-14	Obligations to inform and notify a) Completeness of the information b) Compliance with the time limits c) Form requirements	It should be documented for each processing, where and how these information requirements are fulfilled. This can be done by referencing data protection notices, contract components, disclaimers in forms, with regard to employee data e.g. also by referencing company agreements (which have been communicated internally at the moment of data collection).

Article	Content	Comment
Art. 20	Data portability	It should be recorded whether a claim of the data subject for this procedure exists, and if so for which data categories (if necessary, including any justification). The state of implementation, respectively intended measures should be recorded.
Art. 32	Technical and organizational measures a) Result of the risk assessment b) Possibilities of pseudonymization and anonymization c) Date of the last inspection of the risk assessment	Besides the general descriptions of the technical and organizational measures (see mandatory disclosures), a detailed documentation can be useful for internal management.
Art. 35	Data protection impact assessment a) Necessity b) Result	The result of the examination whether a data protection impact assessment is necessary including a justification should be recorded. Provided that a data protection impact assessment must be carried out, the data protection impact assessment should be documented in detail (see Bitkom guidelines on risk assessment and data protection impact assessment and in the following ↗ chapter 3.1)

Depending on the organizational form and the layout of the IT structures in the company, the data protection officer may recommend any documentation in addition to the mandatory disclosures in the extended record of processing activities. The record of processing activities and the, if necessary, additional information of the specialist departments are the most important tools for the data protection officer for completing his tasks.

It is also recommended to include an overview in the extended record of processing activities that documents the people or groups that have data access.

In the following, some examples of possible further additions are listed that exceed the legal minimum requirements. These statements have proven to be useful in practice, but are not mandatory and should not be comprehended as exhaustive:

- Used hardware and software
- employed processors in the sense of processing on behalf of the controller (if not already evident from the list of recipients)
- interfaces
- safety concepts
- responsible contact persons in the departments

Detailed sample forms for the composition of the public and internal record of processing activities can be found in the annex [↗in 5.1](#)

2.5.4 Internal additional information in the record of processing activities of the processor

From the point of view of the processor, some extended notifications are appropriate in order to ensure and prove compliance with the requirements.

Article	Content	Comment
Art. 28 para 3	Instructions of the controller	Depending on the diversity or customer-specificity of the range of services of the processor, a central documentation of the issued instructions can be useful. References in the extended record of processing activities to instructions that are already employed (even those that are issued aside from the contract) but maybe in different positions can be very useful in practice.
	Deletion procedure	Deletion procedures and records of deletion protocols in the record of processing activities can be useful tools.
Art. 28 para 2	Subcontracts	To ensure compliance with the authorization and communication requirements in relation to the employment of subcontracted processors, the latter should be attributed to each individual processing. Additional documents (e.g. approval of the controller) should be created.

2.6 Definition of a processing activity

The GDPR does not explicitly explain the term “processing activity”. Article 4(2) of the GDPR defines the term with: “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, such as

- The collection
- The recording
- The organization
- The structuring
- The storage
- The adaptation or alteration
- The retrieval
- The consultation
- The use
- The disclosure by transmission
- The dissemination or otherwise making available
- The alignment or

The regular use of the term “processing activity” in various provisions in the GDPR suggests that the term is very broad in its meaning, not just the abovementioned enumeration of the individual steps of processing, but also with regard to separating one activity from another.

This guideline therefore also uses the term “processing activity” broadly, encompassing the entirety of the processing activity, with which one purpose or more purposes shall be realised. Processing activities can include a variety of data processing programs and files. It is essential for the processing activity to determine the pursued purpose of the processing.

In practice, it is important to clarify what exactly a processing activity is and which processing activities must be listed in the processing records.

A tried and tested approach is the evaluation of the focus of the procedures:

- Business processes of the controller (our recommended approach to gain a manageable number of record entries)
- Processing purposes
- Systems, hardware and software

2.7 Form of the processing records

According to Article 30(3) GDPR, the processing records must be kept in writing, but this includes an electronic form.

In addition to the realization of the records on paper or electronically on the basis of word processing, spreadsheet, or database software, the use of specialized software programs is also possible. The appendix shows an overview of the implementation by different suppliers (see [in 5.4](#)) however, these have not yet been evaluated.

When selecting technical implementation measures, the data protection officer will usually have to define the appropriate requirements for the company. Especially the following factors should be taken into account:

- Effective cooperation with the departments
- Usability (if applicable, for the departments)
- Availability and integrity of procedural information

3 Creating the processing records

The creation of the processing records is not the data protection officer’s responsibility, but is to be carried out by the controller (Article 30 of the GDPR). The data protection officer should, however, assume a consultative function within the meaning of Article 39(1) of the GDPR, according to which he shall inform and advise the controller of obligations under the Regulation with regard to all processing activities. Due to his professional knowledge, the data protection officer will, as it was already done in the past, be the one who is assigned the necessary competencies to manage the implementation and data protection assessment of the individual procedures.

The creation of the directory by the controller is typically divided into several phases. It usually starts with a planning phase in which, in addition to the responsibilities and resources required, the necessary methods (e.g. to carry out the risk assessment, the security measures and the data protection impact assessment, see [Risk Assessment & Data Protection Impact Assessment](#)) and corresponding forms / templates are created, illustrations are drafted.

Graphic illustration of an overview of the individual phases

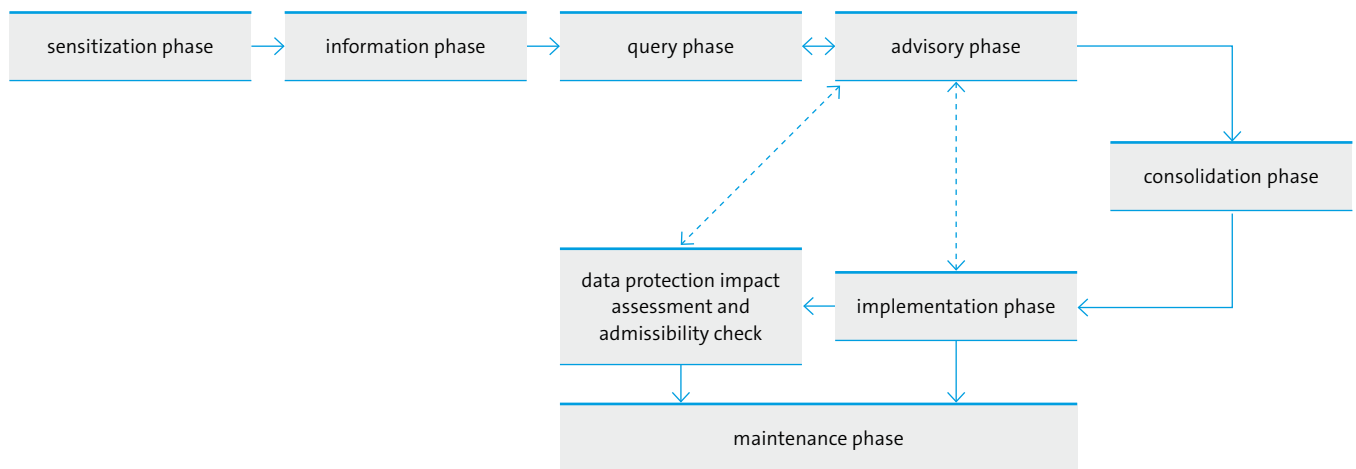


fig 2: Graphic illustration of an overview of the individual phases

3.1 Sensitization phase

As a first step, the departments should be informed about the legal requirements for the creation of the processing records and the related objectives. In order to give the process the necessary importance, the management, as the controller, together with the data protection officer should write a circular letter, and both should sign the letter. The letter should announce the timely start of the process, the processing times should be clearly defined and the responsible staff should be asked to jointly fulfill the task.

Examples of actions by the Data Protection Officer:

- Mailings with information on data protection measures that every employee can observe
- Articles for publication in the intranet
- Information on current articles in the press to raise the general awareness of employees

In practice, information deficits are often found among employees, e.g. that only procedures for the processing of personal data must be included in the processing records.

3.2 Information phase

The employees which are appointed by the departments and who are involved in the preparation of the processing records should be familiarised with the project by talking them through the individual project steps and the forms to be used. It should be made clear that the data protection officer should be informed.

- About the existing application that involve personal data

as well as

- Planned projects or application as soon as possible

Significant changes to existing applications are to be treated as new applications. Whether these are self-developed or externally developed applications is irrelevant.

Examples of actions taken by the Data Protection Officer:

- Preparation of reports and explanations, FAQs, presentations, etc.
- Conducting workshops
- Jointly examining a sample case
- Indication of a negative report (e.g. if the processing does not involve personal data) with a corresponding sample form
- Timely information about the need for a data protection impact assessment, so that all information is available in time for the data protection impact assessment ([↗see 3.7](#))

3.3 Query phase

The best way for the company's data protection officer to receive the necessary information in the most effective way, will depend primarily on the size of the company. In larger companies, for example, detailed questionnaires can be created. The prepared questionnaires can then be sent, with a deadline, to the departments for determining the existing processing activities.

The first thing to evaluate is whether the processing concerns personal data. This includes data which are not identifying a person per se, but which, in combination with other data, can identify a person. If this is not the case, a negative report can be recorded with the sample form.

It may be practical to indicate already known (or typically to be expected in a company) processing that happen within the framework of a business process in advance and to make this list available to the departments for support. The departments then can assign their reports to the indicated processing activities. Additionally, the departments can assess whether there are individual procedures which can be allocated to a common task or whether there are tasks that are already assigned to documented procedures. In this way, the details for the processing records can be determined from the start and the complexity can often be reduced.

For smaller companies, a general and short questionnaire determining the procedures used will often suffice and which can be followed by discussions with the departments for further information collection.

Examples of actions by the data protection officer:

- Distribution of the questionnaires to the departments
- Monitoring of dates by the company's data protection officer

3.4 Advisory phase

During the period of processing of the reporting forms, the departments will, despite all previous information, have numerous further enquiries. In order to handle the queries, a simplified form of a hotline service can be established, depending on the company size. Where there is need for clarification, the disputed points should, where possible, be discussed directly. The aim should be to issue a correct report and, at the same time, to improve the quality of future reports by providing appropriate information.

Examples of actions by the data protection officer:

- Establishing a hotline service
- Scheduling of the necessary time frames for consultation and implementation
- Clarification of open questions or correction of obvious unclear data through direct contact
- Indication of the need for prior checking ([↗see 3.7](#))

3.5 Consolidation phase

The individual processing notifications submitted by the departments are to be structured by the data protection officer. Depending on their size and complexity, they should be condensed and consolidated in order to keep the processing list clear and manageable. In practice, this can e.g. be achieved by collecting the individual processing notifications of a specific field of activity and summarising them in a consolidated version for the task area of a department. It is therefore possible to provide information according to different levels of detail. Through the selected structure, it is possible to present a specific field of activity, e.g. for the supervisory authority. If necessary, individual applications can be referenced.

3.6 Implementation phase

After receiving and structuring the notices and feedback from the departments, these must be verifiably documented in the processing records. The following procedure is recommended to fulfill this task.

Firstly, all notices must be checked for completeness and correctness. If the information is incomplete or incorrect, this must be clarified with the respective department.

In the event of a negative report, it must be checked whether the data provided by the departments can be used to confirm that no personal data are affected. Enquiries regarding such reports may be necessary, otherwise the negative report is to be recorded as such.

When reporting automated processing activities, it is necessary to check whether the existing threats to the rights and freedoms of the affected data subjects have been assessed and evaluated in the context of a risk assessment and whether the technical and organizational measures for the protection of the data are sufficient. If this information cannot be confirmed on the basis of the available information, the controller must carry out a risk analysis in accordance with Article 32 of the GDPR and supplement the missing information.

Also, the data protection officer should not rely solely on the report of the department, but rather check the processing activity itself before it is being included in the processing records, especially if particularly many or particularly sensitive data are processed.

In addition, it must be checked whether individual processing activities are permitted (admissibility test) and whether they are subject to the data protection impact assessment or are excluded from it (Article 35 para 5 of the GDPR). If that is the case, the data protection impact assessment has to be carried out before the processing is released and recorded in the processing records.

If all information is complete and correct, the information must be recorded as a processing activity in the processing records. Whether the notices are stored in paper form in a structured manner or electronically can be determined by the controller.

If software is to be used for this purpose, [Chapter 4](#) contains information on what factors should be considered when selecting a suitable program.

After all notices have been recorded and stored, it is advisable to let the department check the procedure report for correctness and to confirm its correctness by signing the report. In this context, it should be explicitly pointed out that changes to the procedure must be reported to the data protection officer.

3.7 Data Protection Impact Assessment and Admissibility Check

For methodology, see [“Risk Assessment und Data Protection Impact Assessment”](#).

For the methodology, see the guide on “Risk Assessment and Data Protection Impact Assessment”. The term “data protection impact assessment” is defined in Article 35 of the GDPR and provides the obligation of the controller to carry out a data protection impact assessment, prior to the processing, for certain envisaged processing operations. The controller shall seek the advice of the data protection officer when carrying out a data protection impact assessment (Article 35(2) of the GDPR). This allows the data protection officer to advise the controller and his department regarding the implementation of the data protection requirements and evaluate the admissibility of the processing (admissibility test) or assess whether a data protection impact assessment is necessary. Depending on the results of this assessment, coordination and consultation with the departments may be necessary. If the procedure needs to be amended by the department, the process returns to the advisory phase.

Automated processing activities are subject to the legally required data protection impact assessment if the processing is likely to result in a high risk to the rights and freedoms of natural persons due to the nature, scope, context and purposes of the processing, especially where new technologies are used (Article 35(1) of the GDPR). In order to be able to carry out this impact assessment, the controller needs properly prepared processing records. All entries as well as the results of the data protection impact assessment should be documented in a comprehensible manner and stored referencing the particular procedure. The result can also be included in the extended processing records.

3.8 Maintenance phase

Updating the processing records requires permanent contact and sensitization of the departments with the data protection officer, who is dependent on notices regarding changes in the application structure and has to make adjustments in the event of changes to the legal framework. This can only be achieved if he is involved in the relevant IT or business processes. As an accompanying measure, it may be appropriate to appoint an internal auditor to check the timeliness of the procedural notices as part of their routine tests. If there is no process for updating the processing records, an update is recommended at regular intervals, for example once a year.

Alternatively, it can be appropriate to return the existing procedural notifications to the departments responsible to check whether they are up-to-date. In such a test cycle, the departments responsible should then, in addition to the timeliness of the procedural notifications already submitted, check for missing procedural notifications. This examination of the responsible departments must be linked to the control activity of the data protection officer.

In all cases, the departments responsible are to be constantly sensitized to report new procedures to the data protection officer in due time. After all, the data protection officer can only confirm the necessity of the legally required data protection impact assessment and advise on the implementation if he is informed of the procedures prior to their launch.

Examples of actions, e.g.:

- Verification of the actuality of notifications of the departments by the data protection officer or an internal audit
- Obtaining confirmation from the departments that the existing notifications are up-to-date; within regular periods (depending on the company, approximately in one to three years)

4 Software for Managing the Processing Records

The criteria for selecting suitable software to support the creation and maintenance of the processing records depend on the size and direction of the company. The most important criterion is the question whether the software is to be used by the data protection officer alone, or whether other persons will also use and operate the software.

The following part shows an overview of the basic functions each software must include:

- representation of the mandatory data required by Article 30 of the GDPR
- input of additional information to be able to incorporate operational requirements
- Backup of all input data (backup concept)
- Printout of the input data for the compilation of reports
- access protection against unauthorized access of the program
- updateability of the program to take include new requirements or new functions
- adjustable data erasure

Additional functions, which should optionally be offered by the software:

- Illustration of the two roles, the controller and the processor
- user interface should be configurable to be adapted to personal needs
- Possibility to extend and adapt the input fields
- Encrypted data storage
- Possibilities to export the data to word processing programs (MS Office / PDF)
- Integrated online help
- Support by the software manufacturer
- Multilingual user interface
- Configurable reports

If a program is to be operated by several users, e.g. so the respective process managers themselves can create or maintain their own processes, the program should also offer the following:

- the user interface should be intuitive to use
- network capability to give all users access via the internal corporate network
- interface to LDAP or Active Directory (AD) to enable efficient user management
- user- and authorization concept (client capability)
- controllable automatic notifications to the data protection officer when changes are made by the user
- notifications to the users as a reminder/ request to conduct necessary notifications/ actions
- calendar with reminders and notifications (reminder / alarm function)

The appendix [under 5.4](#) shows an overview of some providers.

5 Appendix

5.1 Examples of Processing Records

5.1.1 Example of a processing record of the controller established in the EU

The following information are the legally required minimum requirements, which shall be made available to the supervisory authority on request. (Article 30(4) of the GDPR).

Name and Address of the Controller	Data Protection Officer
Mustermann Marketing GmbH Eckstr. 5 60437 Frankfurt Tel: +49 69 555-4514 E-Mail: info@mustermann-gmbh.de	Mr. Kraus Data Protection Officer E-Mail: dsb@mustermann-gmbh.de Tel: +49 69 555-4512

No. Joint Controllers	Purpose	Group concerned	Category of data	Adresse	Transfer to third country	Erasure time	TOMs	
03	n.a.	Management journey planning	employees	Booking and invoice data, booking preferences, travel times, booking history, legitimization data (credit card number)	Internal travel management, travel agency, service provider travel agency agency, travel service provider (flight, train, hotel), Visa provider, financial accounting	travel to third countries or use of services from third countries	after the expiry of trading and tax related retention requirements	Measures according to the safety protection level, no special measures required according to risk analysis
04	Fleet management	Senior staff, sales representatives	Master data, driving license data, billing data, insurance data, data on special processes, vehicle damage, accidents	Internal fleet management or external service provider, workshop and service partner insurance	Not planned			
05	Marketing and Sales	a) Active and former clients b) Sales prospects c) Website visitors	Reg. a & b: contact and list data, product interests, communication history, credit rating data Reg. a: master and contract data, buying history Reg. c: pseudonymised profiles according to § 15 TMG	Marketing, Sales external service providers,	Transfer of pseudonymised tracking data to US-service provider	Reg. a & b: if revoked by the customer or after 2 years after termination of contract		

No. Joint Controllers	Purpose	Group concerned	Category of data	Addresse	Transfer to third country	Erasure time	TOMs
06	Service provision 1	a) clients b) former clients c) employees d) suppliers	reg a & b: master data, buying and billing data reg c & d: master data, performance record			after the expiry of trading and tax related retention requirements	
07	Service provision 2	a) clients b) former clients c) employees d) suppliers	reg a & b: master data, buying and billing data zu c & d: master data, performance record			after the expiry of trading and tax related retention requirements	
08	Billing	a) clients b) former clients c) employees d) suppliers	reg a & b: master data, buying and billing data zu c & d: master data, performance record	Financial accounting, sales, support	Not planned	after the expiry of trading and tax related retention requirements	
09	Customer service	active and former clients	master-, contract- and service data, invoice data, correspondence, procedure information such as support requests, payment defaults etc.	Financial accounting, sales, support	Not planned	After the expiry of guaranties and warranties,	
10	Purchasing	Employees of suppliers	company contact data, if applicable, information on knowledge and skills	Purchasing department, warehouse	Not planned; depending on the supplier possible in individual cases	after the expiry of trading and tax related retention requirements	
11	Tax and commercial audit trail, financial management	a) clients b) suppliers c) employees d) sales prospects	Master data, service and invoice data	Financial accounting, controlling	Not planned	after the expiry of trading and tax related retention requirements	
12	Business-, Property and information security	Employees, clients, visitors	Master data and pictures for company ID card, authorization, account information, security protocols and authentication data (admittance, approach, access, transfer), results of routine inspections, visitor lists, information reg. room bookings, surveillance videos, licence plate number of private vehicles	Security officer, reception, if necessary, the legal department		12 month after the year in which the data was collected ended; 3 years after termination of employment	

5.1.2 Example of a processing record of representative of a controller established outside of the EU

The following information are the legally required minimum requirements, which shall be made available to the supervisory authority on request (Article 30(4) of the GDPR).

Name and Address of the Controller	Representative in the EU	Data protection officer
Mustermann Marketing Inc. 133 Ferry Morse Way Mountain View, CA 94041 USA Tel: +1 555-4512-3453 E-Mail: info@mustermann.com	Mustermann Marketing GmbH Eckstr. 5 60437 Frankfurt Site Offenbach Senefelderstr. 160 63069 Offenbach Director Frankfurt	Mr. Kraus data protection officer dsb@mustermann-gmbh.de Tel: +49 69 555-4512

No.	Joint Controllers	Purpose	Group concerned	Category of data	Adresse	Transfer to third country	Erasure time	TOMs
01	Mustermann Vertriebs Inc. Mustermann Datacenter Inc.	Applicant management	applicants	Master data, data concerning knowledge and skills such as certificates, résumé, reviews, communication data	Recruiting, departments, financial accounting, participation boards, human resource service provider	USA	Application documents such as certificates, résumé etc: 4 months after completion of application process, with consent of the data subject: 2 years after receiving the application, correspondence: 10 years	Measures according to the safety concept, protection level 1
02	Mustermann Vertriebs Inc. Mustermann Datacenter Inc.	Human resources management	Employees according to § 3 para 11 BDSG	a) master und contract data b) Information about knowledge and skills, such as certificates, résumé and reviews c) Social security data, payment data such as wage data, tax code, denomination d) Bank data e) absence	staff, departments, financial accounting, participation boards, social security, specialists departments, bank	Not planned	3 years after termination of employment, after the expiry of trading, tax and social security related retention requirements	Measures according to the safety concept, protection level 2 additionally: separate access area for staff department

5.2 Example of a processing record of a processor

The processor is also required to maintain processing records, but the information requirements differ.

The following example shows a processing record of a service provider who offers applicant management as Software as a Service (SaaS):⁵⁶

Name and address of the processor ⁵	Data Protection Officer
<p>Mustermann Software GmbH Eckstr. 5 60437 Frankfurt Tel: +49 69 555-4514 E-Mail: info@mustermann-gmbh.de</p> <p>Site Offenbach Senefelderstr. 160 63069 Offenbach</p>	<p>Mr. Kraus Data Protection Officer E-Mail: dsb@mustermann-gmbh.de Tel: +49 69 555-4512</p>

No.	01
controller / employer	Bernd Example Kölner Str. 233 80999 München Tel: +49 89 555-9876 info@bernd-beispiel.de
Categories of processing	Abstract description of the service or services, e.g. applicant management in the form of SaaS or provision and operation of storage capacities
Transfer to third countries	USA (use of a cloud infrastructure provider) <ul style="list-style-type: none"> Data transfer based on standard data protection clauses according to Art. 46 para 2 lit. c) GDPR⁶
Measures according to Art. 32 para 1 GDPR	Measures according to the safety concept + if applicable, additional encryption if agreed upon with the controller


⁵ If established outside of the EU, implementation analogous to 5.1.2.

⁶ Indication of the provided appropriate safeguards is not always required, but generally useful

5.3 Forms for Compiling the Processing Records

The enumerations of explanations regarding the fields and boxes are to be found [in 5.3.4](#)
The forms are also available for [Download](#) as a word version.

5.3.1 Form: recording a processing activity



page 1|9

Recording a processing activity

(please forward to the data protection officer)
Only fill in, if personal data is being processed (Explanation No. 1)

Note: If the space of this form is not sufficient, please add additional attachments.

Date:
 Person completing the form:
 Telephone number:

Description of the processing activity (Explanation No. 2):
Superordinate business process:
Start of the processing activity (Explanation Nr. 3):

Change of existing processing
 New processing
 Cancellation of existing processing (Explanation N. 4)

1. Basic information on processing and responsibility

1.1 Description of procedure
 (Explanation No. 5)

1.2 department:
 responsible manager:
 if applicable, position indicator

1.3 contact person,
 if not responsible manager
 telephone number:

1.4 Name and address of processor, if
 processing on behalf of the controller
 according to Art. 28 GDPR (Explanation No. 6):
 Contract number:

www.bitkom.org



2. Purpose and legal basis of data processing (Explanation No. 7)

page 2|9

2.1 Purpose and legal basis of data processing (Explanation No. 8):

< Text >

2.2 Legal basis (please tick and explain)

Special regulation apart from the GDPR
(please indicate: provision, section, paragraph, subparagraph)
< Text >

Consent of the data subject (Art. 6 para 1 a) GDPR): Please insert
consent clause and consent mechanisms
< Text >

Collective agreements (e.g. company agreement, collective
agreement): (please indicate: exact title, section, paragraph)
< Text >

Justification, execution or termination of employment
(nationally regulated e.g. in the BDSG)
< Text >

Contract or initiation of contract with the data subject
(Art. 6 para 1 b) GDPR)
< Text >

Balancing of interests (Art. 6 para 1 f) GDPR:
Please specify the priority interests
< Text >

3. Circle of groups concerned

Circle of groups concerned (Explanation No. 9)	type of data/ categories of data (Explanation No. 10)	Are special types of data being? (Explanation No. 11)
		<input type="checkbox"/> Yes Which: < Text > <input type="checkbox"/> No
		<input type="checkbox"/> Yes Which: < Text > <input type="checkbox"/> No
		<input type="checkbox"/> Yes Which: < Text > <input type="checkbox"/> No



4. Data transfers and recipients (Explanation No. 12)

page 3|9

4.1 Internal recipients within the controller

Internal department (org-unit) < Text >
 Type of data < Text >
 Purpose of data communication < Text >

4.2 External recipients and third persons (every other recipients, also group companies)

External post < Text >
 Type of data < Text >
 Purpose of data communication < Text >

4.3 Planned data transfer to third countries (established outside of the EU)

Which state < Text >
 Type of data < Text >
 Purpose of data communication < Text >

5. Standard period for data erasure (Explanation No. 13)

Are there legally required retention obligations or other applicable erasure obligations?

- Yes, please indicate which: < Text >
- No

Please describe if and following which criteria the data are erased:
 < Text >

6. Means of processing

Which software or systems are used for processing?

description	manufacturer	functionality	provision
< Text >	< Text >	< Text >	<input type="checkbox"/> internally developed / individual software <input type="checkbox"/> standard- or bought software <input type="checkbox"/> cloud services
< Text >	< Text >	< Text >	<input type="checkbox"/> internally developed / individual software <input type="checkbox"/> standard- or bought software <input type="checkbox"/> cloud services
< Text >	< Text >	< Text >	<input type="checkbox"/> internally developed / individual software <input type="checkbox"/> standard- or bought software <input type="checkbox"/> cloud services



7. Groups with access authorization (simplified authorization concept)
(Explanation No. 14)

page 4|9

description of group	role of authorization	scope of data access (description of types of data)	type of access	purpose
< Text >	< Text >	< Text >	<input type="checkbox"/> read <input type="checkbox"/> write <input type="checkbox"/> erase	< Text >
< Text >	< Text >	< Text >	<input type="checkbox"/> read <input type="checkbox"/> write <input type="checkbox"/> erase	< Text >
< Text >	< Text >	< Text >	<input type="checkbox"/> read <input type="checkbox"/> write <input type="checkbox"/> erase	< Text >

Please explain the process of collecting and managing access authorizations and describe the detailed business authorization concept
< Text > (if necessary, add appendix)

8. Technical and organizational measures (Art. 32 GDPR) (Explanation No. 15)

8.1 Regarding data security measures, the IT-security department was involved
 Yes
 No, if ticked, please explain briefly: < Text >

8.2 Risk Assessment according to Art. 32 GDPR was carried out
 Yes
 No

8.3 Measures of the general internal IT- security concept are appropriate with regard to the assessed risks
 Yes
 No

8.4 Please indicate alternative or additional measures:
 < Text >

availability	< Text >
Integrity	< Text >
confidentiality	< Text >
additional protection for rights and freedoms of data subjects	< Text >



9. Data portability (Explanation No. 16)

page 5|9

Is it possible to export the processed data to the data subject or other services in a commonly used, standardized format?

- Yes, Format: < Text >
- No

10. Information for the data subject (Explanation No. 17)

Where and how are the data subjects, whose data are being processed, informed about the processing?

< Text >

11. Data protection by means of technical design and settings (Explanation No. 18)


Does the processing adhere to the principles of data protection by design and by default?

- Yes
- No

Comments:

< Text >

5.3.2 Form: Notification of a negative report



pagee 1|2

Negative report to record processing activities

(please forward to the data protection officer!)
Only fill in, if personal data is not being processed (Explanation No. 1)
Note: If the space of this form is not sufficient, please add additional attachments

Date:

Basic information on processing and responsibility

1. Person completing the form:
Telephone number:

2. Description of processing activity:
[\(Explanation Nr. 2\)](#)

3. superordinate business process


Change of existing processing
 New processing
 Cancellation of existing processing

4. department:
responsible manager:
if applicable, position indicator:

5. Description of processing data including purpose of processing:

www.bitkom.org

5.3.3 Form for internal confirmation notes of the data protection officer



Form for internal confirmation notes of the data protection officer

Project No., or procedure identification: < Text >

	Date	Name
1. Procedure checked	< Text >	< Text >
2. Notification for the processing records necessary	<input type="checkbox"/> Yes	<input type="checkbox"/> No
3. Data protection impact assessment necessary	<input type="checkbox"/> Yes	<input type="checkbox"/> No
4. If data protection impact assessment is necessary:	result of admissibility check: <input type="checkbox"/> Yes <input type="checkbox"/> No	Comments: < Text >
5. Consultation with the data protection authority necessary:	< Text >	< Text >
6. Data protection filing	< Text >	< Text >

Initiated measures	controller	deadline
1. < Text >	< Text >	< Text >
2. < Text >	< Text >	< Text >
3. < Text >	< Text >	< Text >

www.bitkom.org

5.3.4 Explanation of the forms

Explanation No. 1

According to Art. 4 No. 1 GDPR, “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This comprises name, date of birth, address, income, occupation, licence tag, account or insurance number. Moreover, pseudonymised data, such as an IP-address, that makes the data subject indirectly identifiable are personal data.

Explanation No. 2

Internal identification, the identification of the individual processing allows the attribution to the respective business process in which the data are processed.

Explanation No. 3

Scheduled start of the processing of personal data or actual start. For that matter, the first transmission or storage of data is relevant.

Explanation No. 4

Only to be selected when completing processing. When selected, the original survey form may be used. A decision on the further use of the data, i.e. whether deletion or migration into other processings are required, must be made in consultation with the data protection officer.

Explanation No. 5

Accurate identification of the processing by using commonly used terms and notes for the processing of personal data.

Explanation No. 6

This serves to ensure a careful selection of the service provider, verification of a contract and the exercise of control duties.

Explanation No. 7

Definition of the purpose of the processing of personal data and the statement of the legal basis for the processing (prohibition principle).

Explanation No. 8

Specific description of the purpose of data processing and data processing itself. If possible, it is recommended to determine explanations consistent with the terminology known in the company and, in case of doubt, to consult the data protection officer.

Explanation No. 9

Statement of the groups of data subjects affected by the processing, e.g. staff (employee (-groups)), consultants, clients, suppliers, patients, debtors, policyholders, interested parties.

Explanation No. 10

Examples of data categories: identification- and address-data, contract master data, data on bank or credit card accounts, IT usage data (e.g. connection data, logging information).

Explanation No. 11

The processing of special categories of personal data is regulated in Article 9(1) GDPR. This includes processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Explanation No. 12

Purpose and recipient of personal data for further processing or use within the responsible department or within a transmission to third parties.

“Recipient” means any person or entity receiving data, e.g. contractors, customers, authorities, insurance companies, medical personnel, processor (e.g. service computer centre, call centre, companies responsible for erasing data), or a process or business process to which the data is transferred.

Explanation No. 13

According to Article 5(1)(e) GDPR, personal data shall be kept for no longer than is necessary for the purposes for which the personal data are processed. Taking into consideration (e.g. tax) legislation, statutory or contractual storage periods, the data must be deleted immediately after the purpose for the data processing ceases to exist. The company's data protection officer should be consulted if no deletion is selected or doubts in relation to storage periods and deletion routines exist.

Explanation No. 14

Outline of the authorization procedure and statement of the eligible groups. If available, it can be referred to a comprehensive operational authorization concept.

Explanation No. 15

Description of the protective measures with regard to the control objectives for the respectively processed personal data. Further details on the requirements for protective measures according to Art. 32 GDPR can be found in the in chapter 4.1 of the guideline on

risk assessment and data protection impact assessment. In case of a determined internal safety policy in the company, a reference to the coordination with the organizational unit “IT security” can be made.

In addition, reference can be made to ISO 27001. The eight control targets for appropriate data protection against misuse and loss must not be comprehended as an exhaustive or complete compulsory catalogue of measures. Thus, due to a special legislation on data protection, further control objectives and corresponding measures may be required (e.g. by the

Explanation No. 16

In case of processing on the basis of a contract or consent, for which data subjects have provided the company with data, they have the right pursuant to Art. 20 GDPR to receive the personal data concerning him or her in a structured, commonly used and machine-readable format or to transmit those data to another controller, if technically feasible.

Explanation No. 17

According to Article 12 of the GDPR, the controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 GDPR to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information may be provided in writing or by other means, e.g. by electronic means.

Explanation No. 18

Pursuant to Article 25 of the GDPR, the controller shall implement appropriate means for the processing and appropriate technical and organizational measures which are designed to meet the requirements of the GDPR and to protect the rights of data subjects.

5.4 Providers of Software for Compiling Processing Records

Current state: 28/05/2018

The following part shows an overview of some providers and products that can support the controller when compiling the processing records. The list is not exhaustive and does not represent preferences of the Bitkom Data Protection Working Group. Each controller is required to implement his own quality standards with regard to design and functionality of the products.

Processing records

2b Advice, data protection software:

[↗https://www.2b-advice.com/GmbH-de/Datenschutzsoftware](https://www.2b-advice.com/GmbH-de/Datenschutzsoftware)

(The current version already enables the user to illustrate all aspects of the GDPR. An updated version, which will depict the GDPR with regard to its wording and preset content (including a specific module for managing data protection risks with regard to the impact assessment) is being finalised at this time and will be published in short term.)

Deichmann+Fuchs Business Solutions: DS-GVO – Verzeichnis der wichtigen Verarbeitungstätigkeiten [↗https://www.deichmann-fuchs.de/datenschutz/dsgvo-%E2%80%93-verzeichnis-der-wichtigen-verarbeitungst%C3%A4tigkeiten/dsgvo-verzeichnis-der-wichtigen-verarbeitungstaetigkeiten.artikel.html](https://www.deichmann-fuchs.de/datenschutz/dsgvo-%E2%80%93-verzeichnis-der-wichtigen-verarbeitungst%C3%A4tigkeiten/dsgvo-verzeichnis-der-wichtigen-verarbeitungstaetigkeiten.artikel.html)

d.velop GDPR compliance center:

[↗https://store.d-velop.de/erweiterungen/d.velop-gdpr-compliance-center/](https://store.d-velop.de/erweiterungen/d.velop-gdpr-compliance-center/)

GDPR-notes:

[↗https://www.gdprnotes.de/en/](https://www.gdprnotes.de/en/) (in process)

Sicoda: DSBeasy Software for processing records:

[↗https://www.sicoda.de/dsbeasy-verfahrensverzeichnis-software/](https://www.sicoda.de/dsbeasy-verfahrensverzeichnis-software/)

(according to statement of the provider, the software does implement the requirements of the GDPR)

Otris Privacy group data protection, data protection management-software:

[↗https://www.otris.de/produkte/otris-privacy-datenschutzmanagement/](https://www.otris.de/produkte/otris-privacy-datenschutzmanagement/)

WEKA, data protection, data protection management:

[↗https://shop.weka.de/datenschutz/datenschutz-management-kompakt](https://shop.weka.de/datenschutz/datenschutz-management-kompakt)



Bitkom represents more than 2,600 companies in the digital sector, including 1,500 direct members. With more than 700,000 employees, our members generate a domestic turnover of 140 billion Euros a year, exporting high-tech goods and services worth another 50 billion Euros. Comprising 1,000 small and medium-sized businesses as well as 300 start-ups and nearly all global players, Bitkom's members offer a wide range of software technologies, IT-services, and telecommunications or internet services. They produce hardware and consumer electronics or operate in the sectors of digital media and the network industry. 78 percent of the companies head-quarters are located in Germany with an additional amount of 9 percent in other countries of the EU and 9 percent in the USA as well as 4 percent in other regions. Bitkom supports an innovative economic policy by focusing the modernization of the education sector and a future-oriented network policy.

**Federal Association for Information Technology,
Telecommunications and New Media e.V.**

Albrechtstraße 10
10117 Berlin
T +4930 27576-0
F +4930 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom